Humboldt-Universität zu Berlin
Institut für Informatik

Diplomarbeit

Einsatz elektronischer Signaturen und Zeitstempel für die Sicherung digitaler Dokumente

von
Daniel Ohst

Datum: 01.09.2003

Gutachter: Prof. Dr. Wolfgang Coy
Prof. Dr. Ernst-Günter Giessmann
Dr. Peter Schirmbacher

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

Dieses Verzeichnis enthält Abkürzungen, die im Rahmen der Arbeit verwendet und nicht als allgemein bekannt vorausgesetzt werden können.

Abkürzung	Beschreibung
ASD	Archiv-Sicherungsdatei
DES	Data Encryption Standard
ETSI	European Telecommunications Standard Institute
METS	Metadata Encoding and Transmission Standard
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
PKS	Public Key Service
RSA	Rivest Shamir Adleman
SHA-1	Secure Hash Algorithm 1
SigG	Signaturgesetz
SigV	Signaturverordnung
URN	Uniform Resource Name
ZDA	Zertifizierungsdiensteanbieter

1 Einleitung

In den letzten Jahren haben sich elektronische Publikationen erfolgreich als neue Publikationsform in vielen Gesellschaftsbereichen etabliert. Eine Reihe von Veröffentlichungen erscheint inzwischen ausschließlich in elektronischer Form, z.B. aus Gründen einer hohen sicherzustellenden zeitlichen Aktualität oder auch um den vergleichsweise hohen Kosten einer konventionellen Publikation zu entgehen.

Vor allem im wissenschaftlichen Bereich werden neue Möglichkeiten eröffnet, der interessierten Öffentlichkeit Dokumente zur Verfügung zu stellen, die vorher insbesondere aus Kostengründen nicht oder nur eingeschränkt publiziert wurden, z.B. Forschungsberichte oder andere wissenschaftliche Abschlussarbeiten.

Die Vorteile sind leicht einzusehen. Die ohnehin in elektronischer Form erzeugten Dokumente können auf einem Webserver mit Internetverbindung abgelegt werden. Mit Hilfe von Suchmaschinen oder durch Austausch bzw. Kommunikation der URLs sind die Dokumente interessierten Nutzern zugänglich. Besonders die Schnelligkeit, mit der Informationen damit zur Verfügung stehen, ist eine in vielen Bereichen fast nicht mehr wegzudenkende Erweiterung wissenschaftlichen Arbeitens.

Dennoch erwächst bei genauer Betrachtung auch eine Reihe von Problemen, die sich aus der Nutzung elektronischer Publikationen ergibt. Dazu gehören z.B. der Umgang mit den verschiedenen Dateiformaten der Dokumente, die Aufbereitung für eine effiziente, maschinenunterstützte Recherche, die systematische, bibliotheksgerechte Erfassung von elektronischen Publikationen, Fragen der Sicherung des Urheberschutzes und vieles mehr. Durch die Möglichkeit der Verarbeitung multimedialer elektronischer Elemente, wie Videos oder Audio-Dateien ergeben sich völlig neue Möglichkeiten für Publikationen, die natürlich auch andere Verarbeitungsanforderungen nach sich ziehen.

In den letzten Jahren wurden und es werden bis heute an einer Reihe von Hochschulen in Deutschland Projekte im Kontext elektronischer Publikationen durchgeführt. Zunehmend wird es in der Zukunft darum gehen, die gewonnenen Erfahrungen aus dem Projektumfeld in Regelprozesse- und angebote zu überführen. Hierzu zählen u.a.

- die Übernahme von Prozessen zur elektronischen Publikation in das normale Aufgabenspektrum von Bibliotheken bzw. Rechen- und Medienzentren,

- die Professionalisierung und Erweiterung von Dienstleistungen, wie z.B. Printing on Demand [ProPrint03],
- die Schaffung rechtlicher Rahmenbedingungen für elektronische Publikationen,
- die Standardisierung von Aufgaben des elektronischen Publizierens sowie die Generierung von Referenzlösungen und „Best practice"-Ansätzen.

Die Erstellung und Nutzung elektronischer Publikationen stellt nicht nur eine technologische Herausforderung dar. Vielmehr wird sich auch eine Reihe von traditionellen Arbeitsweisen aller am Publikationsprozess Beteiligten verändern. Dies erfordert eine neue Kultur des elektronischen Publizierens [DINI02]. Der Umgang mit Dokumenten dieser Art wird zu einer Kernaufgabe der Bibliotheken werden.

An der Humboldt-Universität zu Berlin wurde bereits 1997 im Rahmen des Projekts „Digitale Dissertationen" (DiDi) mit dem systematischen Aufbau eines Angebots für die elektronische Publikation von Dissertationen begonnen. Schwerpunkte der Arbeit waren der Aufbau eines zertifizierten Dokumentenservers, die Entwicklung von Workflows zur Handhabung elektronischer Publikationen, eine umfassende Autorenunterstützung und - als herausragendes Projektmerkmal - die frühzeitige Orientierung auf die langfristige Verfügbarkeit der Arbeiten durch Einsatz des Archivierungsformats SGML und die dazugehörigen technischen und organisatorischen Maßnahmen.

Mit dem Beschluss des Akademischen Senats der HU im Jahre 1998 [HUAS98], der grundsätzlich für alle Promovenden die Abgabe ihrer Arbeit auch in elektronischer Form ermöglichte, wurde eine beispielhafte Entwicklung begründet. Bis zum Juni 2003 wurden auf dem Dokumentenserver edoc.hu-berlin.de 581 Dissertationen veröffentlicht. Hinzu kommen zahlreiche andere Publikationen, wie z.B. Diplomarbeiten oder Antrittsvorlesungen. Seit 1999 werden auch alle medizinischen Habilitationen (derzeit 161 auf dem Dokumentenserver) gemäß Habilitationsordnung elektronisch veröffentlicht. Diese Zahlen stellen einen Spitzenwert im Vergleich mit anderen Hochschulen dar und sind ein Indiz für die hohe Akzeptanz der Angebote durch die Autoren. Grund dafür ist sicherlich auch die frühzeitige und enge Zusammenarbeit zwischen Bibliothek und Rechenzentrum, die die Umsetzung der Projektziele wesentlich unterstützt hat. Diese erfolgreiche Arbeit wurde in den Folgejahren durch die Arbeit in weiteren Projekten fortgeführt und ergänzt [EDOC03b].

Schon frühzeitig wurden im Rahmen der Projekte Sicherheitsaspekte beim elektronischen Publizieren berücksichtigt. So werden bereits seit 1998 digitale Signaturen zur Sicherung der eingereichten Dissertationen verwendet.

Einen Schwerpunkt der Forschungstätigkeit stellt die langfristige Sicherung der Verfügbarkeit elektronischer Dokumente dar. Konventionelle papiergebundene Veröffentlichungen können bei entsprechender Lagerung und der Einhaltung gewisser Anforderungen, z.B. an die Papierqualität, durchaus viele Jahre lesbar bleiben. Bei digitalen Dokumenten ist die Lesbarkeit manchmal schon über einen Zeitraum von wenigen Jahren problematisch. Hierzu zählt die beschränkte Haltbarkeit von Speichermedien. Zwar sind die Hersteller in der Lage, durch Berechnungen und Simulationen ungefähre Zeitangaben zu machen. Erfahrungen in der Langzeitarchivierung insbesondere moderner Medien in realen Umgebungen sind jedoch nur eingeschränkt vorhanden. Hier müssen Konzepte entwickelt werden, nach denen Daten vor ihrer physischen Zerstörung auf andere Speicher migriert werden können.

Eine weitere Aufgabe im Rahmen der langfristigen Sicherung ist die Interpretierbarkeit von gespeicherten Daten, d.h. die Verfügbarkeit von Hardware und Software zum Lesbarmachen der Dokumente. Es gelingt teilweise schon nicht mehr, wenige Jahre alte Dateien auf einem modernen Rechner darzustellen, da z.B. die Textverarbeitungssoftware das Dateiformat nicht mehr unterstützt. Eine Konvertierung in neue Formate ist meist mit Informationsverlust verbunden. Es gibt verschiedene Ansätze, dieser Problematik zu begegnen.

Urheberrechtliche und verwertungstechnische Fragen, die sich aus der prinzipiell unbegrenzten und verlustfreien Kopierbarkeit digitaler Dokumente ergeben, sind derzeit Gegenstand z.T. heftiger politischer Diskussionen [UHG03], werden in diesem Rahmen jedoch nicht betrachtet.

Die stetige Zunahme von elektronischen Publikationen, die teilweise schon gar nicht mehr auf konventionellem Weg publiziert werden, erfordert eine intensive Betrachtung aller Fragen der Sicherung der langfristigen Verfügbarkeit, um der bereits vor einigen Jahren in die Diskussion gebrachten „digitalen Amnesie“ [Hirsch96] entgegenzuwirken. So wird es zukünftig auch zu den Aufgaben von Bibliotheken bzw. Betreibern von Dokumentenservern gehören, durch technische Maßnahmen sicherzustellen, dass illegale Manipulationen an elektronisch veröffentlichten Publikationen nicht möglich sind [MWFKBW99].

Im Rahmen dieser Diplomarbeit wird ein Aspekt der langfristigen Sicherung von Dokumenten, nämlich der Nachweis von Authentizität und Integrität, betrachtet. Im Gegensatz zu papiergebundenen Publikationen müssen bei digitalen Dokumenten besondere Maßnahmen ergriffen werden, um auch in vielen Jahren noch nachweisen zu können, dass sie z.B. vom angegebenen Autor stammen und nicht nachträglich verändert wurden.

Im ersten Teil der Arbeit werden grundsätzliche Anforderungen an die Langzeitarchivierung digitaler Dokumente beschrieben und Projekte erwähnt, die sich speziell mit dieser Problematik auseinander setzen.

Im zweiten Kapitel werden die Grundlagen für die Sicherung von Authentizität und Integrität digitaler Dokumente erläutert. Zunächst erfolgt eine Betrachtung der entsprechenden kryptografischen Verfahren und Anwendungen sowie ihrer Umsetzung in technische Standards. Des Weiteren wird die aktuelle Rechtslage, insbesondere beim Einsatz von elektronischen Signaturen, wie sie sich aus dem Signaturgesetz und weiteren Gesetzen und Vorschriften ergibt, dargestellt. Der Abschnitt schließt mit einem Abriss zu aktuellen Problemen und Trends, die derzeitig beim Einsatz von Signaturen zu beobachten sind.

Anschließend wird ein technisches Konzept für die Sicherung von Authentizität und Integrität der digitalen Dokumente entwickelt, die im Rahmen des Publikationsprozesses an der Humboldt-Universität verarbeitet werden. Dabei entsteht eine Architektur, die eine weitestgehend automatische Durchführung des Signatur- und Archivierungsprozesses erlaubt und sich in den bestehenden Bearbeitungs-Workflow eingliedert. Besondere Beachtung wird der Behandlung von mehrteiligen Dokumenten geschenkt, die schon dadurch entstehen, dass Konvertierungen in verschiedene Ziel-Dateiformate durchgeführt werden oder multimediale Bestandteile enthalten sind. Des weiteren werden die konkreten organisatorischen und technischen Anforderungen an die Ausstellung und Nutzung von Zertifikaten sowie die Erstellung von elektronischen Signaturen und Zeitstempeln betrachtet. Ziel ist die Schaffung einer einfachen und nachnutzbaren Lösung, die trotzdem alle hohen Sicherheitsansprüche erfüllt.

Abbildung 1.1 Dokumentenserver der HU Berlin

2 Sicherung digitaler Dokumente

Die folgenden Abschnitte stellen überblicksartig wesentliche Aspekte der Langzeitsicherung digitaler Dokumente dar. Langfristige Sicherung bedeutet, die elektronischen Dokumente über einen Zeitraum zur Verfügung zu stellen, für den aus jetziger Sicht keine sicheren Annahmen zu der dann zur Verfügung stehenden Technik gemacht werden können. Deshalb sind Voraussetzungen zu schaffen, die eine Vielzahl möglicher Wege offen lässt, um flexibel auf geänderte Anforderungen reagieren zu können.
Es werden die wesentlichen Anforderungen an eine langfristige Sicherung formuliert und Lösungsansätze aufgezeigt, die derzeitig Gegenstand der Forschung sind. Anschließend werden einige nationale und internationale Vorhaben aufgeführt, die sich speziell mit dem Thema der Langzeitarchivierung digitaler Publikationen auseinander setzen.

2.1 Langzeitarchivierung digitaler Dokumente

Die Bibliotheken haben den Auftrag, die Publikationen dauerhaft zu archivieren. Schon 1995 hat der Bibliotheksausschuss der DFG formuliert: „Der Erhalt des 'kulturellen und wissenschaftlichen Gedächtnisses' der Gesellschaft obliegt wissenschaftlichen Bibliotheken. Zu ihren klassischen Aufgaben gehören deshalb die Archivierung und die dauerhafte Bereitstellung (Langzeitsicherung) von Literatur und Informationsmaterialien. Dies gilt auch für elektronische Publikationen.“ [DFG95]

Folgende wesentliche Problemstellungen sind bei der langfristigen Sicherstellung der Verfügbarkeit von elektronischen Publikationen zu betrachten.:

1. Sichere Speicherung

   Elektronische Dokumente werden auf Datenträgern, wie z.B. Festplatten und Disketten, gespeichert. Für Sicherungszwecke sind meistens Wechselmedien, wie CD-ROMS, DVDs, DAT- und DLT-Bänder, im Einsatz. Alle diese Medien besitzen je nach Art der Speicherung der Daten eine unterschiedliche Lebensdauer (z.B. bedingt durch die Haltbarkeit der verwendeten Materialien). Das bedeutet, dass die Daten nicht unbegrenzt lange fehlerfrei gespeichert werden können. Während papiergebundene Publikationen bei entsprechender Lagerung und Papierqualität durchaus mehrere Jahrhunderte überdauern können, liegt die Haltbarkeit einer CD-ROM bestenfalls bei einigen Jahrzehnten. Diese Angaben beruhen auf den Angaben der Me-

dien-Hersteller, die die Zeiten aufgrund von Tests oder Simulationen ermittelt haben. Aufgrund der kurzen Zeit, die diese Medien erst zur Verfügung stehen, war bisher natürlich noch keine realitätsnahe Prüfung möglich. Es ist also erforderlich, in regelmäßigen Abständen zu prüfen, ob Medien noch lesbar sind, und bei Bedarf der Inhalt auf neue Medien zu migrieren.

2. Interpretierbarkeit

   Die auf einem Medium gespeicherten elektronischen Publikationen stellen zunächst nichts weiter als einen Bitstrom dar, der mit geeigneter Hardware und Software vom Medium gelesen und anschließend mit einer Applikation unter Auswertung eines definierten Datenformats dem Nutzer sichtbar gemacht wird, z.B. durch Darstellung am Monitor oder als Ausdruck. Aufgrund des rasanten technologischen Wechsels kann jedoch nicht einmal heute mehr sichergestellt werden, dass z.B. ein Textdokument, das mit Wordstar 2.0 erstellt wurde und auf einer 8'' Diskette gespeichert ist, gelesen werden kann.

   Die Forderung ist somit, dass die Daten zunächst einmal korrekt vom Speichermedium gelesen und dann auch noch in ihrer Originaldarstellung präsentiert werden können. Es gibt unterschiedliche Konzepte, um dieses Ziel langfristig zu erreichen (Migration von Daten auf neue Plattformen, Emulation alter Systeme und Applikationen auf neuen, Bewahrung alter Systeme und Applikationen).

3. Authentizität und Integrität

   Bei einer papiergebunden Publikation ist eine Fälschung des Textes relativ schwer durchzuführen und mit verschiedenen technischen Maßnahmen auch gut nachweisbar. Ein elektronisches Dokument kann, wenn nicht besondere Sicherungen erfolgt sind, problemlos geändert werden. Erschwerend kommt hinzu, dass diese Änderungen so gut wie nicht nachweisbar sind, sofern keine besonderen Vorkehrungen getroffen werden. Bei der langfristigen Archivierung von elektronischen Publikationen ist also sicherzustellen, dass diese während ihrer Existenz nicht unerlaubt verändert werden und dass der Urheber des Dokuments bzw. die herausgebende Stelle zweifelsfrei erkannt werden kann.

4. Referenzierbarkeit / Suche

   Für papiergebundene Publikationen gibt es eine Reihe von Methoden, um diese langfristig auffindbar zu machen und zur Verfügung zu stellen. So hat z.B. die Deut-

sche Bibliothek die Pflicht, u.a. alle in Deutschland erscheinenden Publikationen zu archivieren. Die Erschließung erfolgt durch die Erfassung in (elektronischen) Katalogen mit den wesentlichen Merkmalen. Diese Kataloge können entweder online oder direkt in einer Bibliothek abgefragt werden, um z.B. den Standort eines Werkes zu ermitteln. Mit der Vergabe einer ISBN-Nummer lässt sich ein Buch eindeutig referenzieren.

Elektronische Dokumente werden auf Servern gespeichert, deren Namen oder deren der Speicherung zugrunde liegende Ordnerstruktur Änderungen unterworfen sind. Eine URL-Referenz auf ein Dokument ist dann nicht mehr nutzbar. Hier helfen Konzepte wie „Persistent Identifier", also die Zuordnung von eindeutigen Bezeichnern, die durch einen zentralen Dienst auf den konkreten Speicherort referenzieren. Auch wenn elektronische Publikationen im Volltext durchsucht werden können, ist eine Katalogisierung durch Vergabe von Metadaten äußerst sinnvoll, um den Zugriff und den Nachweis zu erleichtern sowie eine Integration mit Verfahren für papiergebundene Publikationen zu erzielen.

Die oben angeführten Themenbereiche stellen nur einige wesentliche Problemstellungen dar, die bei der Archivierung elektronischer Dokumente zu beachten sind. Weitere sind z.B. die Gewährleistung des Urheberschutzes oder Verfahren zur inhaltlichen Bewertung von Dokumenten.

2.2 Projekte mit Schwerpunkt Langzeitarchivierung

In diesem Abschnitt werden einige Projekte bzw. Initiativen vorgestellt, die sich insbesondere mit der langfristigen Verfügbarkeit von digitalen Dokumenten beschäftigen.

2.2.1 InterPares

Das Projekt InterPares (International Research in Permanent Authentic Records in Electronic Systems) ist an der School of Library der University of British Columbia beheimatet. Es ist ein Zusammenschluss von Wissenschaftlern verschiedenster internationaler Organisationen und Vertretern der Industrie, die sich die Aufgabe gestellt haben, gemeinsam Theorien und Methoden für die langfristige Sicherung der Authentizität von

elektronischen Daten zu entwickeln. Das Projekt Interpares 1 wurde von 1999 bis 2001 durchgeführt. Seine wesentlichen Ergebnisse sind die Reports der vier Task Forces zu den Themen: Authentizität von elektronischen Daten, (inhaltliche) Bewertung von elektronischen Dokumenten, Bewahrung elektronischer Daten, Entwicklung von Strategien. Die Berichte sind stark archivarisch geprägt und beschreiben zunächst theoretische Modelle und Vorgehensweisen im Rahmen der Langzeitarchivierung. Es wird eine umfangreiche Terminologie erarbeitet und auf elektronische Daten angewendet.

Mit Interpares 2, das am 1.1.2002 begann, wird das erste Projekt fortgesetzt und auf weitere Themen ausgedehnt. Es ist zum 31.12.2006 befristet. Schwerpunkte des Projekts sind die Erweiterung des Forschungsgegenstands von permanenten elektronischen Daten auf dynamische und interaktive Daten sowie die Betrachtung während ihres kompletten Lebenszyklus. Fallbespiele werden aus Bereich Kunst und Wissenschaft vorgestellt.

Der Schwerpunkt des Projekts ist stark auf die theoretische Ausarbeitung von Aspekten der Langzeitarchivierung orientiert. Die Erkenntnisse müssen in praktisch verwertbare Konzepte umgesetzt werden.

Die Projektergebnisse von Interpares 1 sowie Informationen zu Interpares 2 sind unter www.interpares.org abrufbar.

2.2.2 PADI

Dieses Projekt (Preserving Access to Digital Information) der Nationalbibliothek Australiens wurde bereits 1993 ins Leben gerufen, und zwar auf Initiative von Mitgliedern von Bibliotheken und Archiven, um Richtlinien zu erarbeiten, die die langfristige Verfügbarkeit elektronischer Ressourcen gewährleisten. Wesentliche Ziele von PADI sind

- die Förderung der Entwicklung von Strategien und Richtlinien, um auch langfristig noch auf digitale Ressourcen zugreifen zu können,
- Betrieb einer Website mit Informationen zum Projekt,
- die Unterstützung von Initiativen im Projektumfeld sowie
- Bereitstellung eines Forums zum Austausch von Informationen und die Koordinierung von Projekten und Initiativen im Bereich Langzeitarchivierung

Die Bedeutung von PADI liegt insbesondere darin, eine nationale Initiative zu bilden, die Aktivitäten koordiniert und Unterstützung gibt. Auf der Website werden umfangreiche Informationen zu Entwicklungen im Bereich Langzeitarchivierung bereitgestellt, die einer ständigen Aktualisierung unterliegen. Nähere Informationen zu PADI sind unter der URL http://www.nla.gov.au/padi/ zu finden.

Eine weitere nationale Initiative für die Langzeitarchivierung ist die Digital Preservation Coalition (DPC) aus Großbritannien. Schwerpunkte sind auch hier die Koordinierung von Aktivitäten, die Bereitstellung von Informationen und Foren sowie die öffentlichkeitswirksame Entwicklung des Themas.

2.2.3 Digital Library Forum / Initiative Langzeitarchivierung

Einen ähnlichen Ansatz wie PADI verfolgt das Digital Library Forum, das vom Bundesministerium für Bildung und Forschung sowie der Deutschen Forschungsgemeinschaft gefördert wird. Ziele sind die Bereitstellung eines Informationsangebots zum Thema Digitale Bibliothek, einer Übersicht zu Forschungsaktivitäten und Projekten, einer Datenbank zu Ausschreibungen und Förderprogrammen sowie eines Forums für den Informationsaustausch von Interessenten.

Im Rahmen des Projekts „Langzeitarchivierung digitaler Dokumente in Deutschland: Initialzündung für die Erstellung eines gesamtdeutschen Konzepts“ soll die Gründung einer nationalen Initiative vorbereitet werden. Die Ziele sind im Einzelnen:

- Initialzündung für die Erstellung eines gesamtdeutschen Konzeptes zur Vermeidung von Einzelaktionen und Insellösungen
- Thematisierung und weitestgehende Diskussion von Grundsatzfragen
- Abstimmung und Planung koordinierter Aktivitäten bzgl. Langzeitarchivierung digitaler Dokumente in Deutschland zur kooperativen Bewältigung der Aufgaben
- Erarbeitung von Richtlinien / Empfehlungen für die weitere Vorgehensweise in Deutschland, auch für die Förderpolitik des BMBF
- Einrichtung eines Kommunikationsnetzes unter den Beteiligten

Diese Fragen wurden auf einem Workshop diskutiert. In der Abschlusserklärung heißt es u.a. : „Die Initiativgruppe Langzeitarchivierung wird Konzepte für den Aufbau eines

Kompetenznetzwerkes für Deutschland erarbeiten und dafür eine Kooperationsplattform und eine Kommunikationsstruktur entwickeln. Dazu soll ein Projekt beim BMBF beantragt werden.“ Es wäre wünschenswert, wenn damit in Anlehnung an PADI oder die DPC eine deutschlandweite Koordination der Vorhaben zur Langzeitarchivierung erfolgt. Ausführliche Informationen hierzu sind auf den Webseiten des Digital Library Forums unter http://www.dl-forum.de/Foren/ zu finden.

Weitere Projekte im europäischen Umfeld, die jedoch bereits abgeschlossen wurden, sind NEDLIB (Networked European Deposit Library), das die Entwicklung einer Basis-Struktur für eine vernetzte europäische Bibliothek zum Ziel hatte, sowie CeDars (curl examplars in digital archives). Informationen zu diesen Projekten finden sich auf den Webservern http://www.kb.nl/coop/nedlib/ sowie http://www.leeds.ac.uk/cedars/.

3 Grundlagen elektronischer Signaturen und Zeitstempel

Kryptografische Algorithmen und Verfahren sind ein wesentlicher Bestandteil einer Lösung für die langfristige Sicherung von digitalen Dokumenten. In diesem Kapitel sollen die wesentlichen Begriffe eingeführt werden, die zum weiteren Verständnis notwendig sind. Es folgt eine Übersicht zu den rechtlichen Rahmenbedingungen des Einsatzes dieser Verfahren in Deutschland sowie zu den technischen Standards, die bei ihrer Implementation eingesetzt werden. Abschließend werden aktuelle Einsatzbeispiele sowie Probleme und Trends aufgezeigt.

3.1 Kryptografische Begriffe und Verfahren

Die Kryptografie ist die Wissenschaft vom Entwickeln von Algorithmen und Verfahren für sichere Kommunikation. Im Gegenzug beschäftigt sich die Kryptoanalyse mit Methoden zum Kompromittieren und Brechen dieser Verfahren. Wesentliche Grundanforderungen an sichere Kommunikation, die mit Hilfe kryptografischer Algorithmen erfüllt werden können, sind u.a. :

- Vertraulichkeit (Schutz von Daten vor unberechtigter Kenntnisnahme)
- Integrität (Schutz von Daten vor unberechtigter Veränderung)
- Authentizität (Sichere Identifikation von Kommunikationspartnern)
- Verbindlichkeit (Nichtabstreitbarkeit von Kommunikation)

Die folgenden Abschnitte sollen in knapper Form wesentliche kryptografische Begriffe und Verfahren einführen. Dabei wird Wert auf eine allgemein verständliche Darstellung gelegt, für eine intensivere Betrachtung der zugrunde liegenden mathematischen Grundlagen und Protokolle sei auf [Schneier96] oder auch viele andere Online-Quellen verwiesen. Für eine gute Darstellung der historischen Entwicklung von Kryptoalgorithmen kann [Bauer94] empfohlen werden.

3.1.1 Symmetrische Verschlüsselung

Bei diesem Verschlüsselungsverfahren wird ein Klartext unter Anwendung eines Schlüssels nach einem Algorithmus in einen Geheimtext überführt, der durch die Benutzung

desselben Schlüssels wieder entschlüsselt werden kann. In der digitalen Welt wird ein Schlüssel durch eine Bitfolge bestimmter Länge dargestellt, der nach einem bestimmten Algorithmus mit dem digitalen Klartext verknüpft wird, um den Geheimtext zu erhalten. Da für Ver- und Entschlüsselung ein und derselbe Schlüssel genutzt wird, werden diese Verfahren als symmetrisch bezeichnet. Offensichtlich müssen sich Absender und Empfänger vorher auf sicherem Weg auf den Schlüssel einigen. Die folgende Grafik illustriert ein typisches Ablaufschema einer symmetrischen Verschlüsselung.

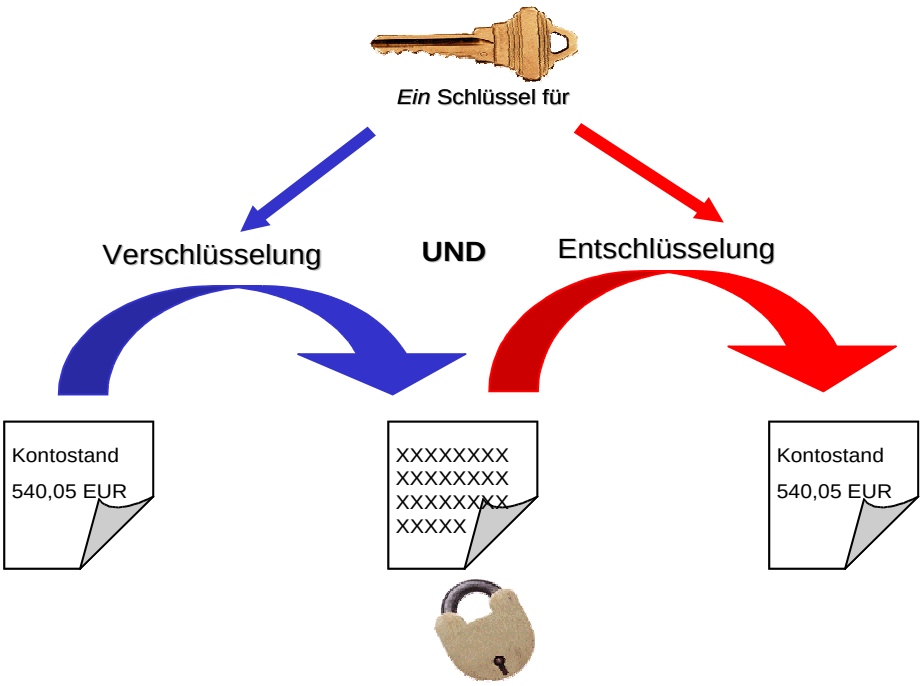


Abbildung 3.1 Symmetrische Verschlüsselung

Ein bekannter Vertreter für symmetrische Algorithmen ist der Data Encryption Standard (DES), der bereits 1977 vorgestellt wurde und mit einer Schlüssellänge von 56 Bit arbeitet. Da diese Länge heute nicht mehr als sicher eingestuft ist, wird eine Variante, der Triple-DES, eingesetzt, der mit zwei oder drei Schlüsseln nach dem Grundalgorithmus arbeitet. Dieser Algorithmus ist lange Zeit der Verschlüsselungsstandard der US-amerikanischen Regierungsbehörden gewesen und soll durch seinen Nachfolger, den Advanced Encryption Standard (AES), der mit Schlüssellängen zwischen 128 und 256 Bit arbeitet, ersetzt werden. Weitere Beispiele sind IDEA, Blowfish, CAST oder RC4.

Symmetrische Verfahren erlauben eine schnelle und bei entsprechender Schlüssellänge sichere Verschlüsselung von Daten. Grundsätzlich problematisch ist die Vorab-Eini-

gung auf einen Schlüssel zwischen je zwei Kommunikationspartnern. Dies kann durch Master-Key-Verfahren (Ableitung von Schlüsseln aus einem Hauptschlüssel) oder durch die nachfolgend beschriebenen asymmetrischen Verfahren gelöst werden.

3.1.2 Asymmetrische Verschlüsselung

Bei dieser Art der Verschlüsselung besitzt jeder Kommunikationspartner ein Schlüsselpaar – einen öffentlichen und einen privaten Schlüssel. Der Absender einer Nachricht verschlüsselt dabei die Daten mit dem öffentlichen Schlüssel des Empfängers, der die Nachricht dann mit seinem privaten Schlüssel entschlüsselt. Das bedeutet, dass der öffentliche Schlüssel problemlos allen Kommunikationspartnern zur Verfügung gestellt werden kann. Die beiden Schlüssel stehen in einer mathematischen Beziehung zueinander, können aber praktisch nicht aus dem jeweils anderen abgeleitet werden. Die folgende Grafik zeigt den Ablauf einer Verschlüsselung und Entschlüsselung.

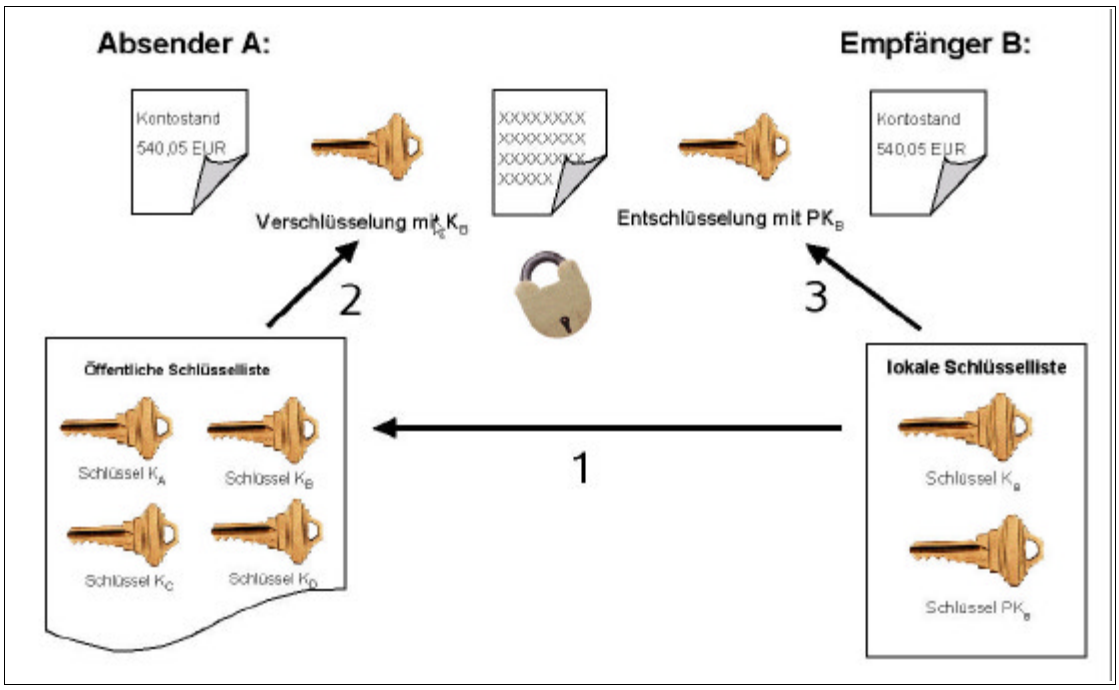


Abbildung 3.2 Asymmetrische Verschlüsselungsverfahren

Der bekannteste Vertreter dieser Algorithmen ist RSA (Rivest, Shamir, Adleman), der mit variablen Schlüssellängen (üblicherweise 1024-4096 Bit) arbeitet.

Asymmetrische Algorithmen haben den Vorteil, dass nur jeweils ein Schlüsselpaar pro Kommunikationspartner benötigt wird; es ist also im Gegensatz zu den symmetrischen kein Schlüsselaustausch vorab notwendig. Allerdings tritt hier das Problem auf, dass der Absender sich auf sichere Weise davon überzeugen muss, dass der ihm vorliegende öffentliche Schlüssel auch tatsächlich der Person des gewünschten Empfängers gehört. Dies wird mit Hilfe von Zertifikaten vertrauenswürdiger Stellen gelöst, die solch eine Zuordnung beglaubigen. Asymmetrische Algorithmen werden häufig für die Realisierung elektronischer Signaturen eingesetzt, wie im weiteren Verlauf des Kapitel beschrieben wird. Des Weiteren arbeiten asymmetrische Algorithmen mit größeren Schlüssellängen und benötigen wesentlich mehr Zeit für die Operationen als symmetrische Algorithmen. In der Praxis wird deshalb häufig die so genannte Hybrid-Verschlüsselung eingesetzt, bei der zunächst ein zufälliger symmetrischer Schlüssel gewählt wird, mit dem die Daten verschlüsselt werden. Anschließend wird nur dieser Schlüssel mit dem asymmetrischen Verfahren übertragen. Die nachstehende Grafik illustriert diesen Vorgang.

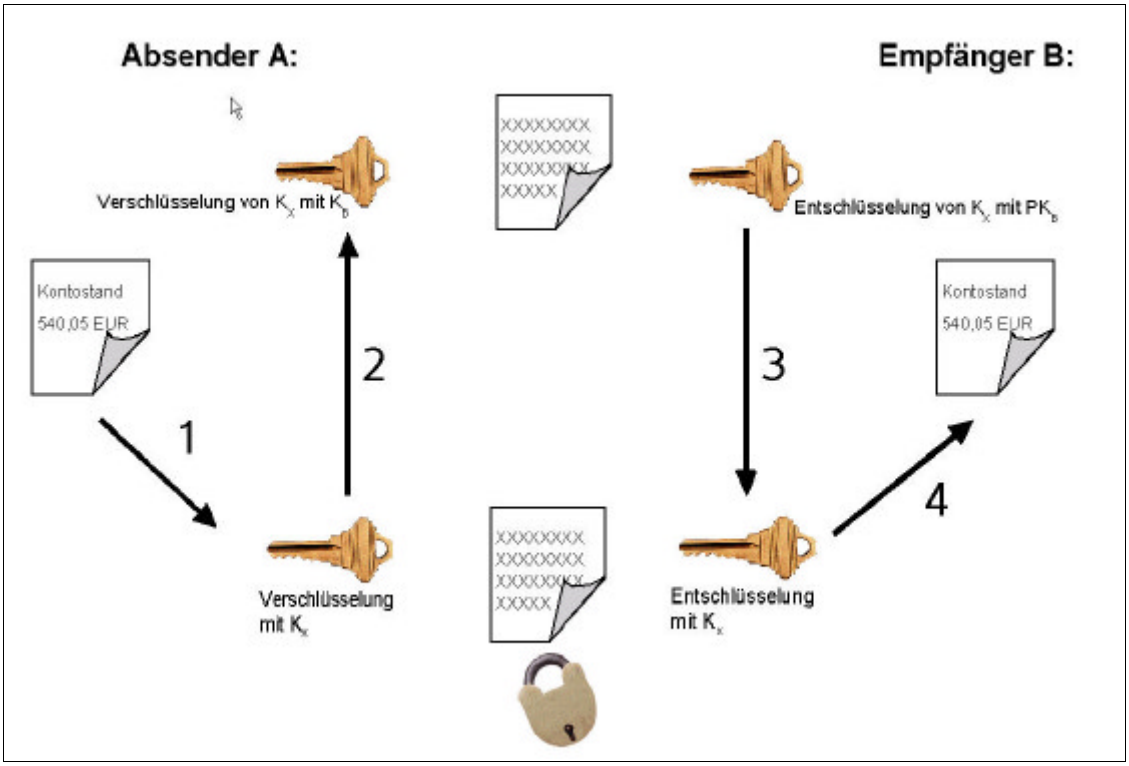


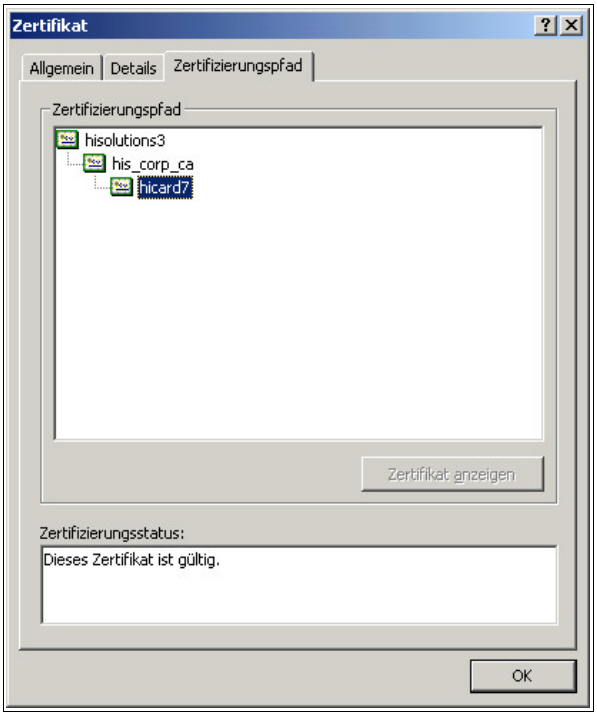
Abbildung 3.3 Hybride Verschlüsselung

3.1.3 Zertifikate

Der Einsatz asymmetrischer Verfahren erfordert ein Schlüsselmanagement, um einen sicheren und effektiven Einsatz zu ermöglichen. Im wesentlichen müssen folgende allgemeine Anforderungen erfüllt werden:

- Realisierung der Bindung öffentlicher Schlüssel an die jeweiligen Inhaber
- Vertrauenswürdige Beschaffung öffentlicher Schlüssel
- Abrufbarkeit von Informationen zu ungültigen Schlüsseln (z.B. nach Kompromittierung)

Zur Lösung werden Public-Key-Infrastrukturen (PKI) mit Zertifikaten eingesetzt. Ein Zertifikat ist eine elektronische Bestätigung bzw. Unterschrift einer vertrauenswürdigen Instanz unter einen öffentlichen Schlüssel einer Person. Diese Instanz wird auch als Certification Authority bezeichnet. Eine Zertifizierung kann auch hierarchisch über mehrere Stufen erfolgen. Ein Zertifikat enthält Angaben zum Aussteller, zum Inhaber, zur Gültigkeitsdauer, zu verwendeten kryptografischen Verfahren sowie Merkmale zur Verwendung des Zertifikats.



Das oberste Zertifikat, das meist selbst durch den Inhaber unterschrieben ist, wird als Root-Zertifikat (im Beispiel *hisolutions3*) bezeichnet. Der Aussteller eines Zertifikats

muss sich in geeigneter Weise von der Identität des Antragstellers überzeugen. Dies kann auf unterschiedlichen Sicherheitsniveaus durchgeführt werden, für eine einfache Identifizierung reicht z.B. die Rückmeldung zu einer E-Mail aus, während für höchste Ansprüche der Antragsteller persönlich unter Vorlage seiner Personaldokumente identifiziert wird. Eine Zertifizierungsinstanz hält weiterhin ein Verzeichnis von zertifizierten öffentlichen Schlüsseln und ein Verzeichnis ungültiger Schlüssel (Certificate Revocation List) bereit.

3.1.4 Hash-Funktionen

Um die Integrität von Daten bei einer Übertragung zu sichern oder auch die Authentizität gegenüber dem Empfänger nachzuweisen, ist eine Operation über der gesamten Datenmenge vielfach zu langsam. An dieser Stelle werden Hash-Verfahren genutzt, die in der Lage sind, ein beliebig großes Dokument auf einen so genannten Fingerprint oder Hash-Wert konstanter Größe abzubilden. Zur Integritätssicherung wird dann nur noch mit diesem Wert gearbeitet. Hash-Verfahren haben folgende grundlegende Eigenschaften:

- Das Originaldokument kann nicht aus aus dem Hashwert erzeugt werden. Dies ist leicht einzusehen, da der Hashwert wesentlich kürzer ist und damit die Information des Originals verloren geht.
- Es ist praktisch unmöglich, zwei Dokumente mit demselben Hashwert zu finden. Das bedeutet, dass selbst zwei Textdateien, die sich nur in einem Byte unterscheiden, vollkommen verschiedene Hash-Werte erzeugen. Selbstverständlich gibt es eine unendliche Anzahl von Paaren von Dokumenten, die denselben Hashwert erzeugen, es ist jedoch äußerst schwer, solche Paare zu finden.

Der heute am häufigsten eingesetzte Hash-Algorithmus ist der Secure Hash Algorithm (SHA-1), der mit einer Länge von 160 Bit arbeitet.

3.1.5 Signaturen

Mit elektronischen Signaturen wird versucht, ein Äquivalent zur eigenhändigen Unterschrift in der digitalen Welt zu schaffen. Wesentliche Funktionen der eigenhändigen Unterschrift sind:

- die Identitätsfunktion (sichert die Identität des Ausstellers),
- die Echtheitsfunktion (garantiert, dass der unterschriebene Text auch vom Unterschreibenden stammt) ,
- die Abschlussfunktion (kennzeichnet den Text als endgültige und verbindliche Version),
- Warnfunktion (Schutz des Unterzeichners vor Übereilung),
- Rechtsverbindlichkeit.

Die elektronische Signatur kann durch Nutzung von asymmetrischen Kryptoverfahren realisiert werden. Im Beispiel des RSA-Verfahrens wird der private Schlüssel des Absender genutzt, um die zu signierenden Daten bzw. ihren Hashwert zu verschlüsseln. Signatur und Klartext werden an den Empfänger übertragen. Dieser nutzt den öffentlichen Schlüssel des Absenders zur Prüfung des empfangenen Dokuments. Hier spielen dann wieder Zertifikate eine Rolle, damit der Empfänger auf geeignete Weise die Identität des Signierers und die Gültigkeit des verwendeten Schlüssels prüfen kann.

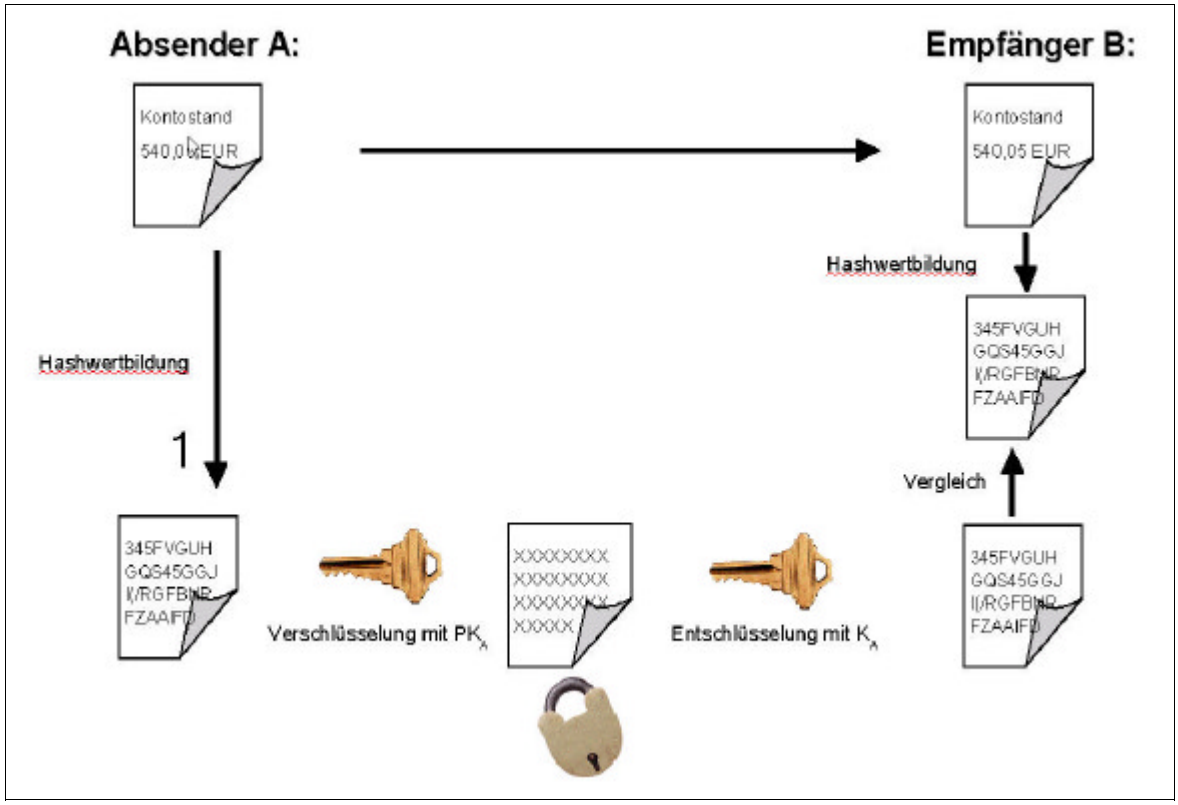


Abbildung 3.4 Elektronische Signatur

Eine spezielle Form von Signaturen sind Zeitstempel. Dabei wird die Signatur unter ein Dokument zusammen mit einer Zeitangabe erzeugt. Der Signierer sollte eine vertrauenswürdige Institution sein, um die Authentizität der Zeitinformation sicherzustellen. Ein Zeitstempel gibt also an, dass das zugrunde liegende Dokument spätestens zum angegebenen Zeitpunkt existiert hat. Damit eignen sich Zeitstempel hervorragend, um Signaturzeitpunkte authentisch festzuhalten, da die Gültigkeitsprüfung von verwendeten Zertifikaten immer auf diesen Zeitpunkt erfolgen muss.

In Bezug auf die anfangs formulierten Eigenschaften der eigenhändigen Unterschrift, kann folgende Bewertung bei Einsatz der elektronischen Signatur vorgenommen werden:

- *Identitätsfunktion*

  Diese wird über das auf einer Chipkarte oder auch nur einer Datei gespeicherte persönliche Zertifikat des Nutzers hergestellt. Die Verwendung des Signaturschlüssels kann erst nach Eingabe einer PIN für eine Chipkarte oder einer Passphrase erfolgen. Eine zweifelsfreie Zuordnung zur signierenden Person kann dadurch nicht hergestellt werden. Eine Chipkarte kann gestohlen und eine PIN ausgespäht oder erpresst werden. Perspektivisch ist der Einsatz von biometrischen Merkmalen denkbar, die eine bessere Personenzuordnung ermöglichen.

- *Echtheitsfunktion*

  Die Echtheit des signierten Dokuments wird durch Prüfung des erzeugten Hash-Werts nachgewiesen. Dieser wird aber im Endeffekt nur über einer Bitfolge erzeugt und sagt nichts über die konkrete Präsentation am Bildschirm aus, die der Signierer gesehen hat. Mögliche Lösungen sind Standardpräsentationen für Dokumententypen [Pordesch01].

- *Abschlussfunktion*

  Durch die elektronische Signatur unter den Hash-Wert des Dokuments lässt sich eine hohe Verbindlichkeit nachweisen. Jede anschließende Dokumentänderung würde bei einer Prüfung sofort bemerkt werden. Wichtig ist jedoch auch wieder die Prüfung dessen, was signiert wurde.

- *Warnfunktion*

  Die Bedeutung einer eigenhändigen Unterschrift ist jedem sofort begreiflich. Niemand gibt seine Unterschrift leichtfertig ab. Die Hemmschwelle ist deutlich geringer,

wenn man nur eine Chipkarte stecken und eine sechsstellige PIN eingeben muss. Zukünftig muss durch technische Maßnahmen sichergestellt werden, dass dem Signierenden die Bedeutung seiner Operationen bewusst ist.

- *Rechtsverbindlichkeit*
  Wie im Abschnitt „Rechtliche Rahmenbedingungen“ in diesem Kapitel noch ausführlicher dargestellt wird, ist mit der Verabschiedung des Formanpassungsgesetzes 2001 die qualifizierte elektronische Signatur der gesetzlich geforderten Schriftform in vielen Fällen gleichgestellt.

3.2 Rechtliche Rahmenbedingungen

Das „Gesetz zur digitalen Signatur“, das am 1.8.1997 in Kraft trat, hatte zum Ziel, Rahmenbedingungen für digitale Signaturen zu schaffen, unter denen ihr Einsatz als sicher gelten kann. Während das Gesetz selbst im Wesentlichen nur Zielvorgaben enthielt, wurden in der gleichzeitig veröffentlichten Signaturverordnung sowie in den Maßnahmekatalogen auch konkrete technische und administrative Vorgaben gemacht. Es wurden jedoch keine rechtlichen oder prozessualen Regelungen verabschiedet. Vielmehr sollte durch die Sicherheitsvermutung des Gesetzes (digitale Signaturen, die die Anforderungen des Gesetzes und der Verordnungen erfüllen, können als sicher gelten) eine Verbesserung im Rahmen der freien Beweiswürdigung vor Gericht erreicht werden.

Das deutsche Signaturgesetz war das erste im EU-Rahmen, jedoch war abzusehen, dass eine Reihe von Ländern eigene Gesetze verabschieden würde. Um die nationalen Vorhaben zu harmonisieren, wurde im Jahre 2000 die „Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen“ [SigRL00] verabschiedet. Die wesentlichen Ziele waren

- die Schaffung einer Basis für einheitliche gesetzliche Signatur-Regelungen in der EU,
- die Stärkung von Vertrauen in die neuen Technologien und Erhöhung ihrer Akzeptanz,
- die Förderung des elektronischen Geschäftsverkehrs
- sowie die Gewährleistung der Freiheit des Binnenmarktes.

Wesentliche Punkte der Richtlinie sind

- die Einführung von drei Klassen von Signaturen (einfache, fortgeschrittene, qualifizierte),
- eine eingeschränkte Technik-Offenheit, die auch Signaturen zulässt, die nicht auf asymmetrischen Verfahren beruhen; Einführung des allgemeineren Begriffs der elektronischen Signatur,
- die Definition von Anforderungen an Signaturerstellungseinheiten und technische Komponenten für Anbieter von Zertifizierungsdiensten und Anwendungskomponenten,
- die grundsätzliche Genehmigungsfreiheit für Zertifizierungsdienste und die freiwillige Möglichkeit der Akkreditierung,
- ein Diskriminierungsverbot für einfache Signaturen,
- eine Gleichstellung der qualifizierten Signatur mit der eigenhändigen Unterschrift, aber keine Regelung zu gesetzlichen Formerfordernissen,
- die Einführung von Haftungsregelungen für Zertifizierungsdiensteanbieter
- sowie Regelungen zur Anerkennung von ausländischer Zertifikaten.

Die Anforderungen der Signaturrichtlinie wurden in dem geänderten Signaturgesetz von 2001 [SigG01] berücksichtigt. Die beweisrechtlichen Vorschriften wurden außerhalb des Signaturgesetzes erlassen. Die wesentlichen Regelungen des neuen Signaturgesetzes werden nachstehend beschrieben.

Die in der Richtlinie aufgeführten drei Klassen von Signaturen werden im Gesetz wie folgt definiert:

- **Elektronische Signaturen**: „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen“. Beispiele hierfür sind eine eingescannte Unterschrift auf einem Fax oder auch nur eine getippte Unterschrift unter einem per E-Mail eingereichten Schriftsatz.

- **Fortgeschrittene Signaturen** sind elektronische Signaturen, die zusätzlich:
  - ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
  - die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
  - mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann,
  - mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

  In der Gesetzesbegründung wird ausdrücklich PGP als Beispiel für fortgeschrittene Signaturen genannt. In neueren Untersuchungen [Rossnagel03b] kommt man jedoch nach genauerer Betrachtung der Anforderungen zu der Schlussfolgerung, dass reine Softwarelösungen im Allgemeinen nur einfache elektronische Signaturen erzeugen können. Fortgeschrittene Signaturen können jedoch z.B. von einer PGP-PKI mit chipkartenbasierter Schlüsselspeicherung erzeugt werden.
- **Qualifizierte Signaturen** sind fortgeschrittene Signaturen, die
  - auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen
  - mit einer sicheren Signaturerstellungseinheit erzeugt wurden.

  Nur für diese Art von Signaturen werden im Gesetz Regelungen und technische Maßnahmen im Rahmen der Signaturverordnung und der Maßnahmenkataloge definiert. Der Begriff des Zertifizierungsdiensteanbieters bezieht sich nur auf Dienste, die qualifizierte Zertifikate ausstellen.

Sichere Signaturerstellungseinheiten sind Software- oder Hardwareeinheiten zur Speicherung und Anwendung des jeweiligen Signaturschlüssels, die bestimmten Anforderungen genügen. Für qualifizierte Signaturen ist dies derzeit die Chipkarte selbst. Signaturanwendungskomponenten sind Software- und Hardwareeinheiten, die Daten dem Prozess der Signaturerstellung zuführen und qualifizierte Signaturen und Zertifikate prüfen können.

Ein qualifiziertes Zertifikat besteht im Wesentlichen aus folgenden Angaben:

- Unverwechselbarer Name oder Pseudonym

- Kryptografische Schlüssel und verwendete Algorithmen
- Gültigkeitszeitraum
- Name des Zertifizierungsdiensteanbieters und Land
- Angaben zur Selbstbeschränkung
- Attribute (berufsrechtliche Zulassung, Vertretung Dritter)

Der Zertifizierungsdiensteanbieter muss den Antragsteller vor der Ausstellung des Zertifikats zuverlässig identifizieren. Dies erfolgt in der Regel durch die direkte Vorlage von Personaldokumenten beim Anbieter oder durch die Nutzung anderer etablierter Verfahren, wie z.B. PostIdent.

Das Signaturgesetz legt weiterhin Anforderungen an den Betrieb eines Zertifizierungsdienstes fest, der grundsätzlich genehmigungsfrei ist. Es muss jedoch ein geeigneter Nachweis der Zuverlässigkeit und der Sachkunde geführt werden. Dies erfolgt durch ein vorzulegendes Sicherheitskonzept, das die Fachkunde der im Betrieb tätigen Personen und die Einhaltung der gesetzlichen Vorschriften und der technischen Vorgaben für die eingesetzten Produkte bestätigt. Dabei können Teilaufgaben eines Dienstes an Dritte ausgelagert werden, wenn diese angemessen in das Sicherheitskonzept einbezogen werden. So nutzen z.B. die Bundesnotarkammern die Infrastruktur des Anbieters Signtrust und übernehmen nur Teilaufgaben, wie z.B. die Registrierung der Antragsteller.
Weiterhin muss der Zertifizierungsdiensteanbieter die geforderte Deckungsvorsorge im Falle einer Verletzung der gesetzlichen Vorschriften oder eines Fehler der eingesetzten Produkte nachweisen. Diese beträgt pro Fall 250.000 EUR.
Für die eingesetzten Signaturerstellungseinheiten sowie für die technischen Komponenten der Zertifizierungsdienste ist die Bestätigung einer gesetzlich anerkannten Prüfstelle, wie z.B. des TÜV-IT, erforderlich. Für Signaturanwendungskomponenten ist eine Erklärung des Herstellers ausreichend.

Zur Erhöhung des Vertrauens in die Dienstleistungen eines Zertifizierungsdiensteanbieters sieht das Gesetz die freiwillige Möglichkeit der Akkreditierung vor. Hierbei wird durch die Behörde oder ein beauftragtes Unternehmen eine umfassende Prüfung der Implementation des Sicherheitskonzepts durchgeführt. Danach erhält der Anbieter ein Gütesiegel und kann sich im Rechts- und Geschäftsverkehr auf die nachgewiesene Si-

cherheit berufen. Die Prüfung wird in regelmäßigen Abständen wiederholt. Die Root-Zertifikate für den Anbieter werden durch die RegTP ausgestellt. Ausgestellte Zertifikate sind noch mindestens 30 Jahre nach Ablauf der Gültigkeit überprüfbar zu halten, im Gegensatz zu 5 Jahren bei nicht akkreditierten. Bei Aufgabe des Diensts oder der Insolvenz des Anbieters sorgt die RegTP für die Übernahme der Verträge durch einen anderen Anbieter.

Auf den Webseiten der RegTP werden Listen mit den akkreditierten Anbietern sowie den Bestätigungen für Hardware- und Softwareprodukte veröffentlicht.

Parallel zum Signaturgesetz wurde die Signaturverordnung [SigV01] erlassen, die detailliertere Vorgaben zur Umsetzung der gesetzlichen Regelungen macht, so z.B. zum Inhalt des Sicherheitskonzepts und der Dokumentation, zur Arbeit von Prüf- und Bestätigungsstellen und zur Prüfung von technischen Komponenten.

Mit dem Formanpassungsgesetz 2001 [FormAnpG01] wurde eine Reihe von Gesetzen ergänzt und geändert, um die Gleichstellung von eigenhändiger Unterschrift und elektronischer Signatur in vielen Bereichen zu erreichen.

In §126 BGB wird festgelegt: „Die schriftliche Form kann durch die elektronische Form ersetzt werden, wenn sich nicht aus dem Gesetz etwas anderes ergibt." Für jene Regelungen, in denen die Schriftform gesetzlich festgelegt wurde, ist §126a ergänzt worden, der bestimmt: „Soll die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden, so muss der Aussteller der Erklärung dieser seinen Namen hinzufügen und das elektronische Dokumente mit einer qualifizierten Signatur nach dem Signaturgesetz versehen". Die Nutzung einer elektronischen Signatur wird für eine Reihe von Fällen explizit ausgeschlossen, wie z.B. für die Ausstellung von Zeugnissen oder die Abgabe von Bürgschaftserklärungen. Dennoch kann eine Vielzahl von Rechtsgeschäften nun auch in elektronischer Form abgeschlossen werden, ohne die Beweiswirkung vor Gericht zu verlieren. Dazu wurde die Zivilprozessordnung geändert, die jetzt in §292 bestimmt: „Der Anschein der Echtheit einer in elektronischer Form (§ 126a des BGB) vorliegenden Willenserklärung, der sich auf Grund der Prüfung nach dem Signaturgesetz ergibt, kann nur durch Tatsachen erschüttert werden, die ernstliche Zweifel daran begründen, dass die Erklärung mit dem Willen des Signaturschlüssel-Inhabers abgegeben worden ist." Während auch einfache elektronische Signaturen als Beweismittel im Prozess im Rahmen der freien Beweiswürdigung beigebracht werden

konnten, wird hiermit für qualifizierte Signaturen eine gesetzliche Vermutung angeordnet. Damit erhöht sich insbesondere für den Empfänger einer Signatur die Sicherheit, da nicht er nachweisen muss, dass die Signatur auf korrekte Weise erstellt wurde. Vielmehr muss der Signaturschlüssel-Inhaber ernstliche Zweifel an der gesetzeskonformen Signaturerstellung vorbringen. Die Prüfung der Signatur nach dem Signaturgesetz besteht im Wesentlichen also darin zu prüfen, ob ein qualifiziertes Zertifikat vorliegt, das zum Zeitpunkt der Signaturerstellung nicht gesperrt war, ob eine sichere Signaturerstellungseinheit und sichere Anwendungskomponenten genutzt wurden. Gegebenenfalls kann auch die Prüfung der technischen Komponenten des Zertifizierungsdiensteanbieters einbezogen werden. Hier zeigen sich dann die Vorteile einer Akkreditierung, da diese Prüfung schon vorab durch die zuständige Behörde durchgeführt wurde. Problematisch ist bei akkreditierten Signaturen die Prüfung auf die Verwendung von bestätigten Anwendungskomponenten, wie sie für akkreditierte Anbieter vorgeschrieben sind. Da es aus technischen Gründen nicht ohne weiteres möglich ist, den Signaturschlüssel-Inhaber zur Nutzung bestätigter Komponenten zu zwingen, ist hier die Sicherheit der zu prüfenden Signatur angreifbar. Nach [Jungermann02] sind diese Faktoren im Rahmen des Erschütterungsbeweises zu berücksichtigen.

3.3 Technische Standards und Regelungen

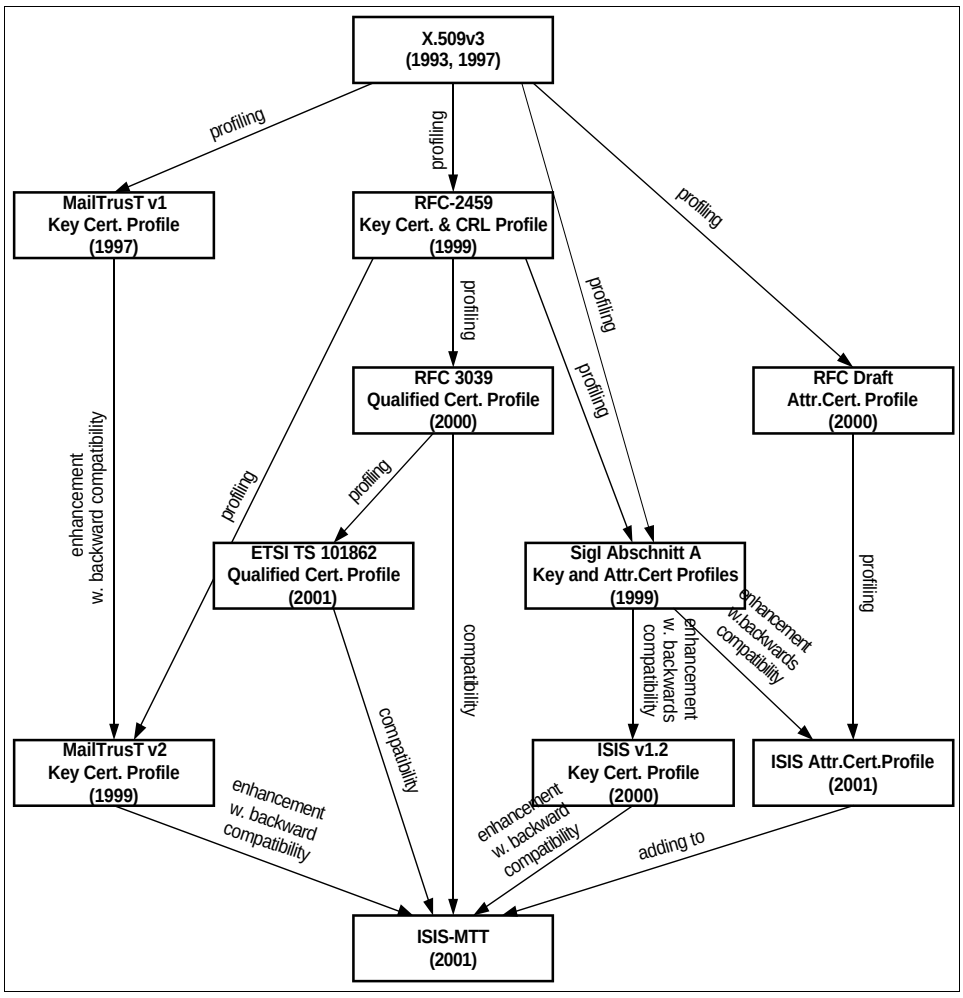
Zur Implementation von elektronischen Signaturen sind vielfältige Festlegungen zu den Strukturen der verwendeten Konstrukte (Zertifikate, Signaturen, Zeitstempel, Verzeichnisse usw.) und zu ihrer inhaltlichen Ausgestaltung als auch zu Prozessen und Kommunikation zwischen verschiedenen Diensten und ihren Objekten zu treffen. Diese Festlegungen erfolgen üblicherweise im Rahmen von Standards verschiedener internationaler und nationaler Organisationen. Der folgende Abschnitt soll nur einen sehr kurzen Überblick zu der Vielzahl existierender Standards sowie Harmonisierungsbestrebungen und neueren Entwicklungen geben.

Die Internet Engineering Task Force (IETF) ist eine der wichtigsten Organisationen im Bereich Internetstandards und veröffentlicht die so genannten RFCs (Request for Comments). Im europäischen Rahmen veröffentlicht das European Telecommunications Standard Institute (ETSI) Standards für den Bereich Telekommunikation, wie z.B. ETSI 101903 zu XAdES (XML Advanced Digital Signatures).

Ein wichtiges Standardisierungsprojekt ist ISIS-MTT, das vom Teletrust-Verein initiiert wurde. Die besondere Bedeutung besteht darin, dass auch die konkrete Implementation von Formaten und Diensten berücksichtigt wird, um eine hohe Interoperabilität zwischen Public Key Infrastrukturen zu erreichen. Die wesentlichen Ziele von ISIS-MTT sind:

- die Auswahl von existierenden technischen Standards, die für das Anwendungsgebiet relevant sind und durch die Nutzer implementiert werden müssen,
- die Reduzierung von Implementationsvarianten um die Interoperabilität zu erhöhen und Kosten für Implementation und Tests zu senken,
- die Ergänzung der referenzierten Standards um Aspekte, die für die Erreichung der Interoperabilität notwendig sind.

Eine Übersicht zu den einbezogenen Standards zeigt die folgende Abbildung (aus [Fiedler03]):



Der Standard bietet trotz der Formulierung von Implementationsdetails durch Profile genügend Gestaltungsspielraum. Des Weiteren wurde ein Testbed für ISIS-MTT entwickelt, das es Anwendungsentwicklern ermöglicht, ihre Produkte auf Standard-Konformität zu testen. Dies hat wesentlich zur Erhöhung der Akzeptanz beigetragen. Die deutschen Trustcenter haben bereits ihren Betrieb auf ISIS-MTT umgestellt oder werden dies noch im Laufe des Jahres tun, was eine wesentliche Verbesserung in der Anwendung elektronischer Signaturen verspricht. So lassen sich dann Signaturen von Fremdanbietern mit der eigenen Anwendung prüfen oder auf einfachere Art und Weise die Dienste mehrerer Anbieter nutzen.

Eine weitere vielversprechende Entwicklung bei Standards für elektronische Signaturen sind XML-Signaturen. XML hat sich in vielen Bereichen als Austauschformat für strukturierte Daten etabliert, z.B. in Business-Workflows zur Datenübertragung zwischen den Prozessschritten. Vorteilhaft ist hierbei die leichte Erfassbarkeit und Flexibilität der XML-Strukturen. So ist es nur folgerichtig, die Möglichkeit zu schaffen, XML-Dateien oder bestimmte Teile davon mit elektronischen Signaturen zu versehen, um während des Prozesses die Authentizität und Integrität transportierter Daten zu sichern. Die XML Signature Working Group hat im RFC 3275 dazu einen entsprechenden Vorschlag unterbreitet. Mit dem ETSI-Standard 101903 wurden XML-Strukturen vorgeschlagen, um die langfristige Verfügbarkeit von Signaturen zu sichern, wie z.B. Erneuerung von Signaturen oder die Speicherung von Prüfinformationen zur Zertifikatskette.

Weitere technische Anforderungen ergeben sich aus dem Signaturgesetz bzw. seinen nachgeordneten Dokumenten, wie der Signaturverordnung oder den Maßnahmekatalogen des BSI. Hier werden konkrete Vorgaben für die Implementation von Diensten und Kriterien für die Prüfung von Komponenten formuliert. So wird z.B. für die Signaturerstellungseinheiten (sofern sie für qualifizierte Signaturen genutzt werden sollen) die Prüftiefe EAL4 oder E3 nach den „Common Criteria for Information Technology Security Evaluation“ bzw. den ITSEC-Kriterien gefordert.
Des Weiteren wird jährlich ein Dokument veröffentlicht, das die Sicherheitseignung von verwendeten kryptografischen Algorithmen für die nächsten Jahre bewertet und das insbesondere für die Langzeitarchivierung von Signaturen bedeutsam ist [BSI03].

3.4 Aktuelle Einsatzbereiche von Signaturen und Zeitstempeln

Obwohl Deutschland mit der Einführung des Signaturgesetzes 1997 schon sehr früh rechtliche Regelungen für elektronische Signaturen formulierte, um ihnen zu einem breiten Einsatz zu verhelfen, ist die Zahl der Nutzer und der sinnvollen Anwendungen bis heute noch als gering einzustufen. Derzeitig arbeiten sechs nach dem Signaturgesetz akkreditierte Trustcenter (Authentidate, Datev, D-Trust, Signtrust, TC Trustcenter und Telesec), die auch eine eigene Infrastruktur aufgebaut haben. Weitere 18 Trustcenter besitzen ebenfalls eine Akkreditierung, nutzen jedoch zu großen Teilen die Infrastruktur der vorgenannten Anbieter und führen selbst im Allgemeinen nur die Registrierungs-Dienstleistungen durch. Somit sind bereits in den letzten Jahren große Investitionen in diesem Bereich vorgenommen worden, die derzeit noch unzureichend durch Anwendungen kompensiert werden.

Während die Nutzung von elektronischen Signaturen bei Privatkunden eher gering ist, nehmen die Anwendungsfelder im Businessumfeld zu. So arbeitet Authentidate, als Spezialist für Zeitstempeldienste, derzeit an Projekten zur automatisierten Erzeugung von qualifizierten Zeitstempeln in Workflow-und Archivsystemen, so z.B. im Bundesministerium für Wirtschaft und Arbeit. Bei der Kaufmännischen Krankenkasse (KKH) wurde die Erfassung der Arbeitgeber-Beitragsnachweise komplett auf die elektronische Archivierung umgestellt, was erhebliche Kosten im Vergleich zur Archivierung der Papierunterlagen einspart.
Während es im Geschäftsumfeld durchaus eine Vielzahl von Projektansätzen aber auch schon erfolgreich umgesetzten Lösungen gibt, ist die Verfügbarkeit von Lösungen für Privatpersonen deutlich eingeschränkter. Dies hat unterschiedliche Ursachen, die im Abschnitt „Probleme und Trends“ noch einmal genauer dargestellt werden. Der Mobilfunkanbieter T-Online bietet seit einiger Zeit die Möglichkeit, sowohl Rechnung als auch Einzelverbindungsnachweis mit einer qualifizierten Signatur versehen elektronisch abzurufen. Diese werden vom Finanzamt anerkannt [StÄndG01]. Dabei muss der Nutzer nicht einmal eine eigene Signaturinfrastruktur besitzen.

Mit dem Projekt Media@komm wird in drei Modellstädten (Bremen, Esslingen, Nürnberg) die virtuelle Stadt modellhaft entwickelt. Ein Teilbereich umfasst auch die Ausgabe von Chipkarten zur Erzeugung von qualifizierten Signaturen an die Bürger, damit diese Dienstleistungen der Behörden auch auf elektronischem Wege in Anspruch nehmen können. So sind über 100 Anwendungen von der Beantragung von KfZ-Kennzei-

chen bis zu Bauanträgen online durchführbar. Die Signaturkomponenten werden den Bürgern hierbei zum stark ermäßigten Preis von 15 EUR zur Verfügung gestellt.

Es existiert noch eine Reihe weiterer Projekte, die größtenteils jedoch Pilotcharakter in kleinen Nutzergruppen haben, wie z.B. der Zugriff auf Rentenkonten der BfA.

Um die Nutzung elektronischer Signaturen voran zu bringen und dabei alle relevanten Partner zu beteiligen, wurde am 3. April 2003 das „Bündnis für elektronische Signaturen" gegründet. Die Gründungspartner stammen aus den Bereichen Öffentliche Verwaltung, Banken, Versicherung, Trustcenter und Pilotprojekte. Ziele des Bündnisses sind

- die Schaffung eines investitionsfreundlichen Klimas auf Basis gemeinsamer Standards für Anwendung elektronischer Signaturen
- sowie die Entwicklung realistischer Geschäftsmodelle für interoperable Infrastrukturen und wirtschaftliche Anwendungen

Die Ziele sollen durch Umsetzung so genannter Konvergenzziele erreicht werden:

- Standardkonformität der Komponenten (PKI-Dienste, Chipkarten, Chipkartenleser, PKI-Anwendungen)
- Multifunktionale Chipkarte
- Einheitliche Sicherheitsniveaus für PKI-Anwendungen
- Ermöglichung des Einsatzes qualifizierter Signaturen

Die Ziele sollen bis Ende 2005 erreicht werden. Jeder Teilnehmer entscheidet jedoch selbst darüber, wie und in welchen Schritten dies durchgeführt wird. Das Bündnis wird mit anderen Initiativen oder Projekten, wie z.B. mit D21 oder E-Government SAGA, koordiniert. Banken und Sparkassen sehen sich aufgrund ihrer langjährigen Erfahrungen im Bereich Karten-Rollout in der Lage, auch für ihre Kunden Chipkarten mit Signaturfunktionalität anzubieten. Die Ausgabe ist schon im Rahmen von Pilotprojekten erfolgt, die EC-Karte soll um Chips erweitert werden, die auch Signaturen erzeugen können.

Die Nutzung von elektronischen Signaturen ist erst an wenigen Hochschulen vorgesehen oder schon eingeführt. Die Universität Dortmund versieht die im System ELDORADO veröffentlichten Hochschulschriften mit digitalen Signaturen für die PDF-Dokumente [UBDO03]. Im Archiv-System MONARCH der Technischen Universität

Chemnitz werden mehrere Hash-Werte für Dokumente erzeugt und mit einer PGP-Signatur versehen. An der HU Berlin werden qualifizierte Signaturen mit Anbieterakkreditierung verwendet, um die archivierten Dateien zu sichern. Die Empfehlungen der Deutschen Initiative für Netzwerkinformation (DINI) sehen ebenfalls die Nutzung gesetzeskonformer Signaturen für die Dokumentensicherung vor [DINI02].

3.5 Aspekte der Langzeitarchivierung elektronischer Signaturen

In vielen Anwendungsbereichen ist es notwendig, Dokumente über einen langen Zeitraum aufzubewahren. Dies ergibt sich oft schon aus gesetzlichen Regelungen. Im Übrigen sind Dokumente so lange aufzubewahren, wie der Inhalt eine vertragliche oder eine andere rechtliche Wirkung entfalten kann.

Elektronische Signaturen und die zugrunde liegenden Dokumente müssen genau wie papiergebundene Publikationen ebenfalls einem Archivierungsprozess unterworfen werden. Im Kapitel 2 wurde bereits die Problematik der Langzeitarchivierung von digitalen Dokumenten kurz angerissen, hier sollen spezielle Aspekte betrachtet werden, die sich für Signaturen ergeben.

Die kryptografischen Algorithmen, die die Basis für die Implementation elektronischer Signaturen darstellen, können im Laufe der Zeit ihre Sicherheitseignung verlieren. Zum einen besteht die Möglichkeit, dass durch die ständig steigenden Rechenkapazitäten oder die optimierte Implementation von Algorithmen die verwendete Schlüssellänge nicht mehr ausreicht, um eine Brute-Force-Attack zu überstehen. Hierbei werden systematisch alle möglichen Schlüssel ausprobiert, was vielfach durch verteilte Rechnernetzwerke realisiert wird. So konnte z.B. ein 56-Bit Schlüssel bei DES-Verschlüsselung im Jahre 1999 schon nach 23 Stunden ermittelt werden. Im selben Jahr wurde ein 512-Bit Schlüssel für RSA ermittelt, für den allerdings gute fünf Monate Rechenzeit erforderlich waren [Clayton01]. Die Verlängerung eines Schlüssels lässt jedoch den Aufwand für seine Ermittlung exponentiell steigen. Die RegTP veröffentlicht einmal pro Jahr ein Dokument, in dem sichere Algorithmen und empfohlene Schlüssellängen für die jeweils kommenden sechs Jahre aufgeführt werden [RegTP03a]. So ist z.B. RSA mit 1024 Bit noch als ausreichend sicher bis Ende 2008 angesehen. Die Empfehlung lautet allerdings schon heute, Schlüssel mit 2048 Bit einzusetzen.

Eine andere Möglichkeit des Verlusts der Sicherheitseignung, ist das vollständige oder teilweise Brechen des Algorithmus. Die hier verwendeten Algorithmen basieren auf schwer, d.h. nur mit exponentiellem Aufwand, lösbaren Problemen, so z.B. der Primzahl-Faktorisierung. Auch wenn derzeit keine Methoden zur effizienten Berechnung bekannt sind, bedeutet dass nicht, dass es nicht möglich ist. Die Wahrscheinlichkeit dafür ist jedoch sehr gering. Es lässt sich für viele Fälle mathematisch nicht beweisen, dass es keine bessere Berechnungsmöglichkeit gibt.

Unabhängig von der Sicherheitseignung von Algorithmen müssen zur langfristigen Prüfbarkeit von Signaturen auch die Prüfvoraussetzungen erfüllt sein, z.B. sind Gültigkeits- und Sperrinformationen zu Zertifikaten verfügbar zu halten. Dies kann durch eine entsprechende Gewährleistung des Zertifizierungsdiensteanbieters erfolgen, der im akkreditierten Fall Zertifikate noch mindestens 30 Jahre nach Gültigkeitsende aufbewahren muss, oder durch zeitgestempelte OCSP-Antworten.

Es ist also möglich, dass eine heute mit einem 1024-Bit-Schlüssel erzeugte Signatur in 10 Jahren nicht mehr als gültig anzusehen ist, da sie zu diesem Zeitpunkt mit einem vergleichsweise geringen Rechenaufwand gefälscht werden könnte. Die Signatur ist also rechtzeitig vorher mit einer größeren Schlüssellänge oder einem anderen Algorithmus neu zu signieren.

Nach §6 (1) SigG hat ein Zertifizierungsdiensteanbieter seine Kunden darüber zu unterrichten, dass Signaturen bei Bedarf zu erneuern sind. Die SigV führt hier weitere Details aus: „Die Daten sind unter Einschluss der alten Signatur mit einer neuen qualifizierten Signatur und einem qualifizierten Zeitstempel zu versehen.“ Es herrscht inzwischen Einigkeit darüber, dass - obwohl das Gesetz hier von Signatur und Zeitstempel spricht - ein qualifizierter Zeitstempel ausreichend ist, da er ja auch nur eine spezielle Art der Signatur darstellt (vgl. [RossnagelFDPB03c]). Dies ermöglicht die Auslagerung des Vorgangs der Neusignatur an einen externen Dienstleister, da kein Zugriff auf die Originaldokumente erforderlich ist. Falls der genutzte Hash-Algorithmus unsicher wird, ist ein Zugriff auf die Dokumente nötig, um einen neuen und sicheren Hashwert zu erzeugen. Um das Risiko zu minimieren, durch die wegfallende Sicherheitseignung eines Algorithmus aufwändige Prozeduren durchführen zu müssen oder sogar den Beweiswert von Signaturen zu verlieren, gibt es Konzepte für den Einsatz multipler Kryptografie, wie z.B. in [Maseberg02], wo dies am Beispiel einer Fail-Safe PKI demonstriert wird.

Es existieren verschiedene Ansätze zur technischen Realisierung der Langzeitsicherung von Signaturen. Eine recht neue Entwicklung sind die XML Advanced Digital Signatures (XAdES), die im ETSI-Standard 101903 definiert sind. Hierbei werden verschiedene Möglichkeiten beschrieben, mit XML-Signaturen Prüfinformationen für Signaturen abzubilden, z.B. komplette Zertifikatsketten oder Gültigkeitsinformationen mit Zertifikaten, die durch Zeitstempel abgesichert sind.
In Deutschland hat sich das Projekt „Archisig" besonders mit dem Thema Langzeitarchivierung von Signaturen beschäftigt. Das Projekt, das im medizinischen Umfeld angesiedelt ist, hat es sich zum Ziel gesetzt, Archivierungs-Technologien so zu erweitern, dass eine langfristige Prüfbarkeit elektronischer Signaturen ermöglicht wird. Es werden Systemarchitekturen dafür entwickelt und prototypisch umgesetzt. Im Rahmen des Projekts ist ein Konzept für die signaturgesetzkonforme Erneuerung qualifizierter Signaturen entwickelt worden[BrandnerP03].

3.6 Probleme und Trends

Wie bereits in den vorangegangen Erläuterungen teilweise angedeutet wurde, ist die Nutzung elektronischer Signaturen derzeit nicht unproblematisch. Eine Vielzahl technischer, organisatorischer, rechtlicher und auch kultureller Fragen ist zu beantworten, um ihnen zu einer breiten Nutzung zu verhelfen. Einige dieser Probleme und eine mögliche zukünftige Entwicklung sollen in diesem Abschnitt aufgezeigt werden.

Wesentlich für den Erfolg elektronischer Signaturen wird die Verfügbarkeit von sicheren und dennoch einfach zu bedienenden Anwendungskomponenten unter Berücksichtigung einer sicheren Signaturerstellungsumgebung sein. Der akkreditierte Zertifizierungsdiensteanbieter TC Trustcenter hat gerade den Auftrag vom BSI erhalten, Anforderungen an eine Standard-PC Umgebung zu definieren, die eine sichere Erstellung von Signaturen erlaubt [TC03]. Dies ist von besonderer Bedeutung, da im Gegensatz zu den Signaturerstellungseinheiten (Chipkarten) sowie den technischen Komponenten für Zertifizierungsdienste der ZDA die Anwenderumgebung nur sehr eingeschränkt kontrollieren werden kann. Es ist aber sicherzustellen, dass z.B. keine Daten auf dem Weg von der Anwendung zur Chipkarte manipuliert werden oder durch so genannte „Trojaner" die Anwendung während des Signiervorgangs manipuliert wird.
Die Anwendungen sollte eine Präsentation von Standard-Dateiformaten integrieren, um dem Nutzer transparent zu machen, welcher Inhalt eigentlich signiert wird. Des Weite-

ren sollten die technischen Interoperabilitäts-Standards umgesetzt sein, um auch Signaturen von Fremdanbietern prüfbar zu halten. Eine Prüfung sollte auch möglich sein, ohne dass der Empfänger einer Signatur selbst einen Signaturschlüssel besitzt.

Vielfach wird der Schutz des privaten Schlüssels auf der Chipkarte durch die PIN kritisiert, da dies keine besonders hohe Sicherheit darstellt. Eine PIN kann bei entsprechender krimineller Energie durch technische Verfahren, aber auch durch einfaches Ausspähen oder andere „Social Engineering"-Verfahren [Mitnick03] in Erfahrung gebracht werden. Das Merken einer Zahl mit 6 Stellen stellt keine besonders hohe Bindung der Person des Besitzers an den Signaturschlüssel dar. Geeigneter ist die Nutzung biometrischer Merkmale, wie z.B. eines Fingerabdrucks oder auch der eigenhändigen Unterschrift, die entsprechend digitalisiert als Identifikation dienen kann.

Die derzeitig von Trustcentern eingesetzten Infrastrukturen sind nicht ohne weiteres interoperabel, d.h. die vom Trustcenter A ausgestellte Signatur hat nicht zwingend ein Format, das eine Gültigkeitsprüfung mit Anwendungen von Trustcenter B ermöglicht. Dies gilt auch für Zertifikate, Zeitstempel oder andere Strukturen. Wünschenswert ist es jedoch, auch Signaturen von Fremdanbietern prüfen zu können und dabei auf Sperrlisten oder OCSP-Responder zugreifen zu können. Hier verspricht der Standard ISIS-MTT Abhilfe, der inzwischen weitgehend akzeptiert ist [Fiedler03]. Alle deutschen akkreditierten Trustcenter haben eine Umstellung in diesem Jahr schon durchgeführt oder werden sie noch abschließen. Es bleibt abzuwarten, ob dann tatsächlich Anwendungskomponenten zur Verfügung stehen, die diese neuen Möglichkeiten auch nutzen können.

Das Problem der Langzeitarchivierung von Signaturen und mögliche Lösungen wurden bereits ausführlicher angesprochen. Auch hier ist zu erwarten, dass sich Standards für die Archivierung etablieren werden und marktreife Produkte zur Verfügung stehen. Um in den entsprechenden Fällen Neusignaturen in großem Umfang durchführen zu können, werden sich Dienstleister am Markt etablieren, die dies professionell anbieten. Um z.B. den Beweiswert von Signaturen zu erhalten, muss sich der Empfänger der Signatur beizeiten darum kümmern, mit neuen Algorithmen zu signieren. Da er u.U. nicht einmal die Infrastruktur zur Erzeugung von Zeitstempeln oder zum Berechnen neuer Hash-Werte besitzt, wird er hier das Angebot dieser Dienstleister in Anspruch nehmen.

Gegenwärtig hat ein Anwender noch einige Hürden zu überwinden, um elektronische Signaturen nutzen zu können: Es sind zunächst umfangreiche (papiergebundene) Antragsformulare zur Identifizierung auszufüllen, zusätzlich werden ein Chipkartenleser

und die entsprechende Anwendung benötigt. Dies ist mit Kosten verbunden, die durchschnittlich 100 EUR betragen. Hinzu kommt eine meist jährlich zu entrichtende Gebühr für die Nutzung der Dienste des ZDA. In Anbetracht der derzeit geringen Anzahl der für die meisten Nutzer zugänglichen Anwendungen, wie z.B. Online-Banking, ist es nicht verwunderlich, dass bisher nur eine absolute Minderheit im Besitz einer Chipkarte mit einem Signaturschlüssel ist. Das ließe sich ändern, wenn diese Funktionalität zusätzlich dort angeboten wird, wo heute schon eine hohe Marktdurchdringung herrscht, sei es durch gesetzliche Grundlage, wie z.B. bei einem elektronischen Personalausweis, oder bei Mobiltelefonen, von denen inzwischen über 40 Millionen in Deutschland existieren. Denkbar wäre, dass der hier sowieso schon vorhandene Chip um Signaturfunktionen erweitert wird, die dann mobil genutzt werden könnten. Eine zuverlässige Identifizierung der Personen ist durch das Antragsverfahren der Mobilfunkdienstleister bereits heute weitgehend gewährleistet. Schließlich ist die breite Nutzung von Signaturen aber an die Verfügbarkeit sinnvoller Anwendungen geknüpft, die den Bürgern einen spürbaren Vorteil bringen.

Ein weiterer Kritikpunkt ist eine mögliche juristische und technische Überregulierung der elektronischen Signatur. Durch die vielen Vorschriften des Signaturgesetzes und seiner nachgeordneten Regelungen, wie z.B. den Maßnahmenkatalogen, wird versucht, ein durchgängig sehr hohes Sicherheitsniveau zu erreichen. Dies kann jedoch eine Etablierung von Lösungen, basierend auf qualifizierten, Signaturen erschweren. Vielfach wird diskutiert, ob nicht auch fortgeschrittene Signaturen mit eventuellen Erweiterungen ein ausreichendes Sicherheitsniveau bieten, vor allem dann, wenn sie von besonders vertrauenswürdigen Institutionen, wie z.B. Banken, herausgegeben werden. Dass die breite Nutzung qualifizierter Signaturen offenbar nicht unproblematisch ist, zeigt auch das Beispiel „ELSTER-Signatur“, bei dem Steuererklärungen digital signiert beim Finanzamt abgeliefert werden können. Hier sind so genannte „qualifizierte Signaturen mit Einschränkungen“ ausdrücklich im Rahmen einer Übergangsphase zugelassen. In der Begründung zur Änderung der Abgabenverordnung heißt es: „Die bei einer 'qualifizierten elektronischen Signatur' erforderliche kostenpflichtige Einschaltung einer Zertifizierungsstelle sowie die unzureichende Verbreitung und Nutzung der dafür erforderlichen sicheren Signaturerstellungseinheit (Kartenleser) dürften zumindest in der nahen Zukunft den angestrebten zügigen Aufbau der elektronischen Kommunikation zwischen den Steuerpflichtigen und der Finanzverwaltung noch erheblich behindern. Ins-

besondere würde die Weiterentwicklung des Projekts ELSTER (Verzicht auf Steuererklärungen in 'Papierform') gefährdet.“

Auch beim Thema Einreichung von elektronischen Rechnungen beim Finanzamt wird vielfach das geforderte Sicherheitsniveau kritisiert. Während dort die Abgabenordnung eine qualifizierte Signatur fordert, brauchen Rechnungen in Papierform z.T. nicht einmal handschriftlich unterschrieben werden oder müssen – bis zu einem bestimmten Rechnungsbetrag – nicht einmal den Namen des Empfängers enthalten. Ähnliches gilt für die Einreichung von vorbereitenden und bestimmenden Schriftsätzen bei Gericht [Splittgerber03].

Es ist zu erwarten, dass in den kommenden Jahren weitere Änderungen am Signaturgesetz vorgenommen werden, um den Erfahrungen aus der Praxis Rechnung zu tragen.

4 Konzept für die Sicherung von Publikationen auf dem Dokumentenserver der HU Berlin

Wie bereits im Kapitel 2 dargestellt worden ist, umfasst das Thema Langzeitarchivierung von digitalen Dokumenten eine Reihe von Aspekten. In diesem Rahmen wird ein Konzept vorgestellt, wie elektronische Signaturen und Zeitstempel genutzt werden können, um die Authentizität und Integrität der Veröffentlichungen auf dem Dokumentenserver der HU Berlin langfristig zu gewährleisten. Die Betrachtungen erfolgen am Beispiel der elektronischen Dissertationen, da sie die mit Abstand größte Gruppe von Publikationen ist. Eine Erweiterung auf andere Publikationsformen ist jedoch problemlos möglich.

4.1 Aufgabenstellung

Folgende Teilaufgaben werden im Rahmen der Konzeption betrachtet:

1. Analyse und Bewertung des derzeitigen Prozesses (Wie ist die Effizienz des aktuellen Systems zu beurteilen? Welche Schwachpunkte gibt es?)
2. Entwicklung eines technischen Konzepts für die Sicherung der Authentizität und Integrität der Dokumente unter Berücksichtigung der derzeitigen praktischen Erfahrungen. Die entstehende Lösung soll sich weitestgehend in die derzeitigen Strukturen und Abläufe integrieren und kurzfristig umsetzbar sein.
3. Beschreibung der notwendigen Schritte für die Erstellung und Nutzung von Signaturen und Zeitstempeln (Hierzu gehören Anforderungen an den Archivserver und seine Einsatzbedingungen sowie alle Fragen zur Beantragung der benötigten Zertifikate.
4. Entwicklung einer Migrationsstrategie für die bereits ausgestellten Signaturen und Zeitstempel
5. Beschreibung von Geschäftsvorfällen im Rahmen des Bearbeitungs-Prozesses und Vorgabe von technischen und organisatorischen Rahmenbedingungen
6. Bewertung der vorgeschlagenen Lösung und Aufzeigen von Optimierungsmöglichkeiten und Weiterentwicklungen

4.2 Ausgangslage

Basierend auf dem Beschluss des Akademischen Senats 1998 wurden in Zusammenarbeit zwischen CMS und UB der Humboldt-Universität die organisatorischen und technischen Grundlagen für die elektronische Abgabeform geschaffen. Dies erfolgte anfangs insbesondere im Rahmen der Projekte „Digitale Dissertationen (DiDi) und Teilprojekt 3 von „Dissertationen Online". Um die Ergebnisse der Projekte langfristig zu sichern und weiter zu entwickeln, wurde die „Arbeitsgruppe Elektronisches Publizieren" geschaffen:

Zu den wichtigsten organisatorischen Aufgaben der Arbeitsgruppe gehören:

- Der Aufbau und die ständige Verbesserung eines Geschäftsprozesses, der von der Abgabe der Dissertation bis zur Veröffentlichung und Archivierung der relevanten Dokumente reicht. Hierzu gehört auch die Definition von Rollen, die innerhalb des Prozesses bestimmte Aktionen durchführen.
- Die Überführung der Tätigkeiten im Rahmen dieses Prozesses vom Projekt- in den Regelbetrieb von CMS und UB, sowie die Erarbeitung von Richtlinien und Standards für die Durchführung dieser Tätigkeiten.
- Die Erstellung von Dokumentationen, die Durchführung von Schulungen, die persönliche Betreuung von Autoren sowie andere Maßnahmen, um den Autoren aber auch den Betreibern der zugrunde liegenden Infrastruktur die technischen Anforderungen an die elektronischen Publikationen zu vermitteln.

Technisch orientierte Aufgaben der Arbeitsgruppe sind u.a. :

- Die Evaluierung, Erarbeitung und Verbesserung von Standards und Standardprodukten im Rahmen des elektronischen Publizierens (Dazu gehören u.a. Standards für Dateiformate, Metadaten, Geschäftsprozesse, Archivierungssysteme sowie die Dokumentensicherung)
- Die Erstellung von Programmen oder Vorlagen für die reale Umsetzung dieser Standards in konkrete IT-Systemarchitekturen
- Der Betrieb der technischen Infrastruktur für die Publikation und Archivierung elektronischer Dokumente
- Die Entwicklung und der Betrieb von Workflow-Anwendungen zur IT-technischen Unterstützung des definierten Geschäftsprozesses

Ein Kernaspekt des an der Humboldt-Universität angewendeten Verfahrens ist neben der Publikation von Dokumenten in einem layoutorientierten Format wie PDF die Konvertierung der Originaldateien des Autors in das struktur-orientierte Format SGML/XML. Dies weist insbesondere Vorteile bei Archivierungs- und Recherchefragen auf. Ein Schwerpunkt des Publikationsverfahrens resultiert deshalb in der Beschäftigung mit Fragen der Konvertierung von Standard-Textverarbeitungsformaten, vorzugsweise MS Word, in SGML/XML auf der Basis einer vorgegebenen Dokumenttyp-Definition (DTD).

Ein weiterer Schwerpunkt, der schon sehr früh als wichtiger Aspekt im Rahmen des Publikationsprozesses erkannt wurde, ist die Frage der Sicherheit von elektronischen Dokumenten und den zugrunde liegenden IT-Systemen. Im vorangegangenen Kapitel wurde der Einsatz elektronischer Signaturen und Zeitstempel für die Sicherung von Dokumenten motiviert. Bereits seit 1998, also mit dem Erscheinen des Signaturgesetzes in seiner ersten Fassung, wurden am CMS Signaturen auf der Basis von Zertifikaten eines akkreditierten Zertifizierungsdiensteanbieters (Telesec) eingesetzt. Dazu wurden für diejenigen Mitarbeiter des CMS, die berechtigt sind, Signaturen über Dokumenten zu erstellen, persönliche Chipkarten beantragt. Die Zertifikate wurden auf Pseudonyme ausgestellt und mit einer Selbstbeschränkung versehen. Durch Nutzung der Anwendung PKS-Crypt der Telesec werden an bestimmten Stellen des Geschäftsprozesses Signaturen und Zeitstempel über den relevanten Dokumenten erzeugt. Dies findet auf einem separaten Archivserver statt, der für die Zeit der Nutzung der Signaturkomponenten einen Netzzugang besitzt. Nach erfolgreicher Durchführung der Aktion wird ein Backup des Servers erstellt und der Rechner komplett abgeschaltet.

Ziel dieses Abschnittes ist die Darstellung der sicherheitsrelevanten Teile des derzeitigen Geschäftsprozesses sowie deren Evaluierung. Aufgrund der Anforderungsanalyse im ersten Abschnitt dieses Kapitels sowie der erkannten Probleme bzw. Unzulänglichkeiten des jetzigen Verfahrens lässt sich im Weiteren eine fortgeschrittene Architektur für die Sicherung der elektronischen Dokumente entwerfen.

Die folgende Abbildung stellt einen Ausschnitt aus dem Publikationsprozess dar und referenziert im Wesentlichen nur die Stellen, an denen sich Dokumentformate ändern bzw. Signaturen oder Zeitstempel über den Dokumenten erstellt werden.

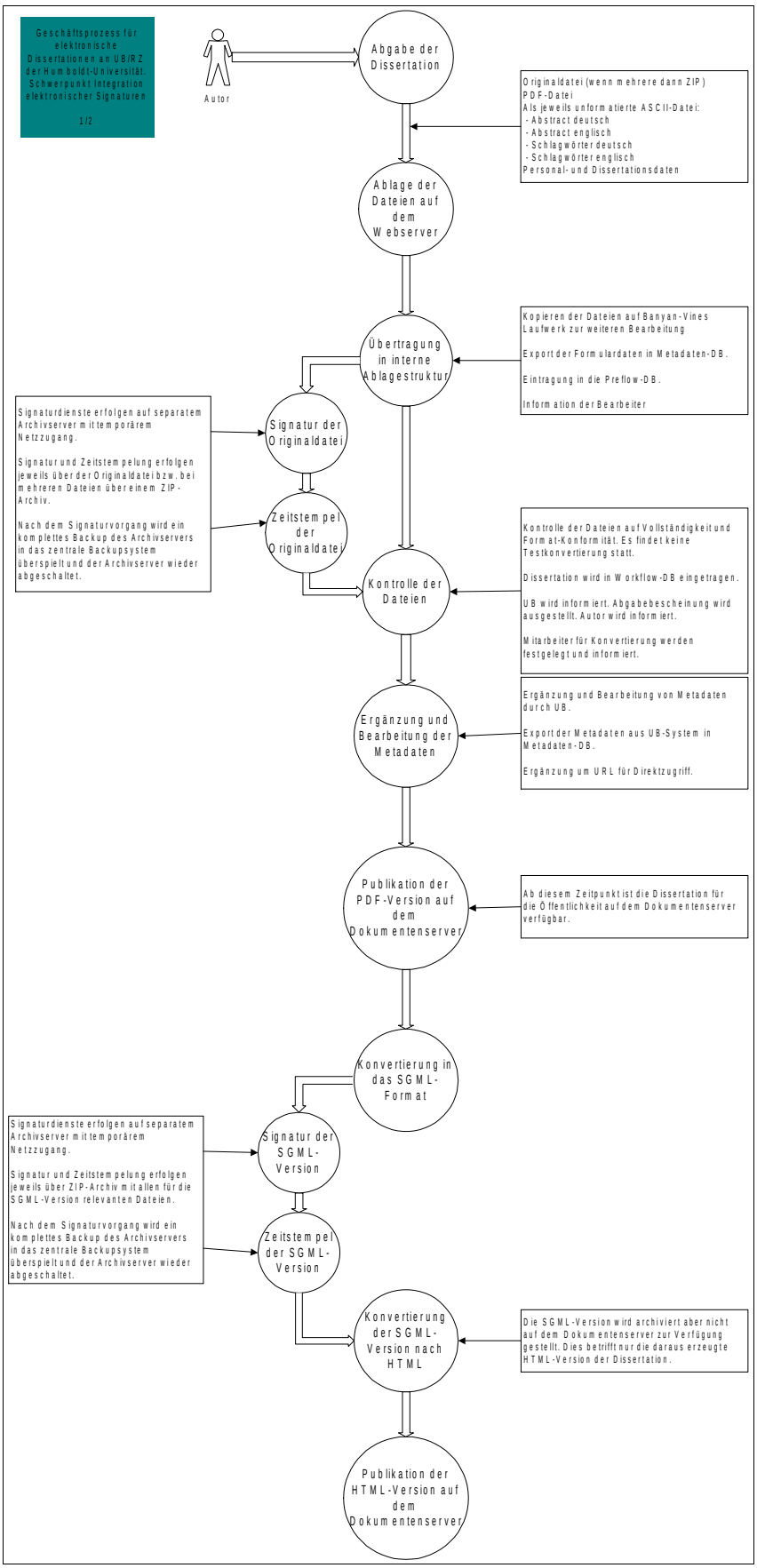


Abbildung 4.1Dokumenten-Workflow

Im Folgenden werden die Kritikpunkte am derzeitigen Verfahren aufgeführt:

1. Im Rahmen des Publikationsprozesses durchläuft ein Dokument eine Reihe von Konvertierungen, die zu folgenden Gruppen zusammengefasst werden können: Das Originaldokument, das durch den Autor abgegeben wird, die PDF-Version, die ebenfalls noch vom Autor erzeugt wird, die SGML-Version und evtl. zusätzliche Dokumente sowie die HTML-Version. Diese Versionen bestehen im Allgemeinen aus mehreren Dateien. Für die Erstellung der Signatur werden sie in einem ZIP-Archiv zusammengefasst und dann signiert. Da in dem derzeitigen Signaturformat auch die Originaldatei vorhanden ist, wurde in einigen Fällen die erhaltene Signaturdatei manuell gesplittet, in dem der intern vorhandene Header und der Footer in separaten Dateien gespeichert und nur diese archiviert wurden. Ein Prüfen der Signatur erfordert dann zunächst ein Zusammensetzen zur Originaldatei.
Die Nutzung einer ZIP-Datei für die Zusammenfassung der Dokumenten-Version ist insofern problematisch, als dass keine Prüfung der Integrität von einzelnen Dateien möglich ist. Entweder muss das ZIP-Archiv für die Signatur-Validierung vorhanden sein, oder es muss aus allen Einzeldateien neu erstellt werden, was schwierig ist, da z.B. durch die Verwendung unterschiedlicher Programme oder auch nur bei Nutzung anderer Kompressions-Level unterschiedliche Archive entstehen, zu denen dann die Signatur nicht passt.

2. Ein nicht direkt aus der Darstellung erkennbarer Aspekt ist die Art der Zertifikate, die im Rahmen des jetzigen Prozesses verwendet werden. Sie werden - konform zum Signaturgesetz - immer für eine natürliche Person ausgestellt. Das heißt, dass bei den derzeit verwendeten Zertifikaten bei einer Prüfung nicht erkennbar ist, welche Institution eigentlich hinter der Person steht, die die Signatur erzeugt hat. Einsichtig ist, dass eine Signatur der Person „Anja Mustermann“ erst dann für das Verfahren relevant ist, wenn z.B. ihre Rolle als Mitarbeiterin der Universitätsbibliothek oder des Computer- und Medienservice erkennbar ist. Nur in dieser Eigenschaft ist sie berechtigt, die Signaturen zu erzeugen. Im Rahmen des Lösungskonzepts ist also eine Möglichkeit vorzusehen, diesen organisatorischen Bezug abbilden zu können.

3. Bereits in den jetzt genutzten Zertifikaten wird eine Selbstbeschränkung in Form eines Attributzertifikats verwendet: „Das Zertifikat dient ausschließlich der Erzeugung digitaler Dokumente der Humboldt-Universität zu Berlin.“ Diese Formulierung ist insofern nicht korrekt, als dass zum einen die Erzeugung von Signaturen und nicht allge-

mein von digitalen Dokumenten gemeint ist und dass Signaturen natürlich nicht von Zertifikaten, sondern von Signaturschlüsseln erzeugt werden. Die Intention der Selbstbeschränkung war sicherlich, dass die Nutzung des Signaturschlüssels auf die Erstellung von Signaturen digitaler Dokumente der HU Berlin beschränkt sein soll. In der Konzeption ist ein Vorschlag für eine Neuformulierung zu unterbreiten.

4. Die derzeitigen Zertifikate wurden auf das Pseudonym „Dig. Dissertationen" ausgestellt. Die Nutzung eines Pseudonyms ist sinnvoll, da es dem Empfänger einer Signatur wenig weiterhilft, wenn er bei der Prüfung nur den Namen eines ihm persönlich meist unbekannten Mitarbeiters der HU findet. Allerdings ist die derzeitige Formulierung zu einschränkend, da sie sich nur auf einen Teil der Publikationen des Dokumentenservers bezieht. Besser wäre ein organisatorischer Bezug und eine Referenz auf das Gesamtangebot elektronischer Publikationen.

5. Es wird derzeit keine zentrale Dokumentation über die ausgestellten Zertifikate und die Erzeugung von Signaturen und Zeitstempeln geführt. Dies ist jedoch zum Nachweis einer ordnungsgemäßen Tätigkeit im Rahmen des Publikationsprozesses erforderlich. Zur Erhöhung der Transparenz sollten auch über die Policy hinaus die Arbeitsgrundsätze für die Erstellung und Nutzung von Signaturen formuliert und veröffentlicht werden.

4.3 Lösungskonzept

4.3.1 Überblick

Das Lösungskonzept gliedert sich in die folgenden Bereiche:

1. Es werden die zu sichernden Daten im Rahmen der elektronischen Veröffentlichung einer Dissertationen festgelegt. Zum Nachweis der Authentizität und Integrität der verarbeiteten Daten werden elektronische Signaturen und Zeitstempel eingesetzt.
2. Ein Archivierungspaket wird entworfen, das zu signieren und zu zeitstempeln ist. Dieses Paket verweist auf zu sichernde Daten und bezieht Änderungen, wie sie z.B. durch Aktualisierung von Metadaten auftreten, ein. Es wird eine Möglichkeit vorgeschlagen, das Präsentationsproblem beim Signieren von Daten zu berücksichtigen.
3. Es wird ein Anbieter von Zertifikaten und die benötigte Software zur Erstellung der Signaturen ausgewählt. Weiterhin werden Anforderungen an die Systemumgebung für den Rechner definiert, auf dem die Signaturen erzeugt werden sollen.

4. Diejenigen Stellen des derzeitigen Geschäftsprozesses zur Publikation von Dissertationen, die sicherheitsrelevante Aktionen durchführen, werden identifiziert und, wenn notwendig, dem neuen Konzept angepasst.

5. Bei der langfristigen Nutzung von Zertifikaten und elektronischen Signaturen kann eine Reihe von Ereignissen, wie z.B. das Ablaufen der Gültigkeit eines Zertifikats, oder die Kompromittierung des privaten Signaturschlüssels eintreten, die bestimmte Aktionen notwendig machen. Diese Ereignisse werden benannt und entsprechende Maßnahmen vorgeschlagen.

6. In Form einer Policy werden Vorschriften zum Umgang mit den erzeugten Signaturen erstellt und die zu dokumentierenden Ereignisse definiert.

7. Es wird ein Verfahren vorgeschlagen, die bereits in der Vergangenheit ausgestellten Signaturen und Zeitstempel in die neue Architektur zu integrieren.

4.3.2 Festlegung der zu sichernden Daten

Im Rahmen des Geschäftsprozesses zur Publikation von Dissertationen werden folgende Gruppen von Daten erzeugt bzw. verarbeitet:

1. Vom Autor eingereichte Dateien
2. Die PDF-Version der Dissertation
3. Die SGML-Version der Dissertation
4. Die HTML-Version der Dissertation
5. Erzeugte Metadaten

Die vom Autor einzureichenden Dateien umfassen gemäß den Anforderungen der „Arbeitsgruppe Elektronisches Publizieren“ der HU [EDOC02a]:

- Originaldateien des verwendeten Textverarbeitungsprogramms (in den meisten Fällen wird es sich hier um Winword-Dateien handeln). Des Weiteren gehören hierzu alle weiteren Bestandteile der Dissertationen, wie z.B. nicht integrierte Bilder, Videos, Audios oder Programme.

- Die durch den Autor erzeugte PDF-Version der Dissertation. Diese wird ohne weitere Änderung auf dem Dokumentenserver publiziert. Bei Problemen ist sie durch den Autor oder in Zusammenarbeit mit dem CMS neu zu erzeugen.
- Jeweils eine Datei mit Schlagwörtern in deutscher und englischer Sprache als unformatierter ASCII-Text.
- Jeweils eine Datei mit dem Abstract der Dissertation in deutscher und englischer Sprache als unformatierter ASCII-Text.

Die SGML-Version entsteht durch automatische Konvertierung der Originaldateien des Autors. Diese müssen den technischen Vorgaben des CMS entsprechen, was in den meisten Fällen durch die Verwendung der angebotenen Formatvorlage realisiert wird. Des Weiteren entsteht ein gewisser manueller Nachbearbeitungsaufwand. Diese Version wird nicht auf dem Dokumentenserver veröffentlicht, sondern dient Zwecken der Recherche und Archivierung.

Die HTML-Fassung der Dissertation wird durch eine automatische Konvertierung aus der SGML-Version gewonnen und auf dem Dokumentenserver publiziert. Hierbei wird die Seiten-Identität der Arbeit gewährleistet, d.h. die Originaldatei, die PDF-Version und die HTML-Version sind auf Seitenebene identisch und damit zitierfähig.

Es lassen sich somit fünf verschiedene Gruppen von Dateien identifizieren, die jeweils zu sichern und zu archivieren sind. Die Inhalte der Gruppen können sich dabei überlappen. Dies sind:

- **Original**

  Hierunter fallen alle vom Autor dem CMS übergebenen Dateien, also die Originaldateien aus dem verwendeten Textverarbeitungssystem (meist MS Word, aber auch LaTeX) inklusive der benötigten Styles u.ä., die durch den Autor zu erzeugende PDF-Datei der Arbeit, nicht integrierte Anhänge, wie z.B. Programme, Audiodateien und ggf. auch Bilder) sowie die geforderten Dateien mit Metadaten und Abstract.

- **PDF**

  Die PDF-Version wird durch den Autor selbst erzeugt und nach Prüfung auf Korrektheit durch die Mitarbeiter des CMS auf dem Dokumentenserver veröffentlicht. Falls hier Fehler bemerkt werden, muss die Version durch den Autor neu erstellt werden.

Hinzu kommen eventuell Anhänge zur Arbeit, die nicht in das PDF integriert werden können, wie z.B. Programme oder Videos.

- **SGML**

  Die SGML-Version wird durch die Mitarbeiter des CMS mit Hilfe von Tools aus den Original-Dateien des Autors (meist MS Word) erzeugt. Die Erstellung dieser Version stellt das Kernstück des Ansatzes der HU zur Archivierung von digitalen Dokumenten dar, da hiermit versucht wird, ein nicht proprietäres Dateiformat für die Langzeitarchivierung zu nutzen. Die SGML-Version wird nicht direkt auf einem Dokumentenserver veröffentlicht, sondern dient vielmehr nur der Archivierung und der Recherche. Auch hierzu gehören wieder Anhänge, die nicht integriert, sondern aus den Dokumenten verlinkt sind.

- **HTML**

  Die HTML-Version wird direkt aus der SGML-Version erzeugt und auf dem Dokumentenserver veröffentlicht. Dabei entstehen einzelne Dateien, die über eine zentrale Einstiegsseite verlinkt sind. So gibt es z.B. separate HTML-Dokumente für die einzelnen Kapitel, das Inhaltsverzeichnis, den Lebenslauf usw. Hinzu kommen die bereits bei der SGML-Version erwähnten Anhänge, die aus dem HTML heraus referenziert werden.

- **Metadaten**

  Hierunter fallen nicht nur die grundsätzlich zu archivierenden Bestandteile der Arbeit, sondern vielmehr Daten, die der bibliothekarischen Erfassung dienen. Dazu gehören die vom Autor eingereichten Dateien mit Schlagwörtern und Abstract in deutscher und englischer Sprache, aber auch während des Publikations-Workflows erstellte Metadaten.

4.3.3 Auswahl des Zertifizierungsdiensteanbieters

Für die Nutzung von elektronischen Signaturen ist eine Reihe von Voraussetzungen nötig, deren technische Grundlagen im Kapitel 3 erläutert wurden. Dazu gehört z.B. die sichere Erzeugung von Schlüsselpaaren, die Ausstellung und Sperrung von Zertifikaten oder der Betrieb von Verzeichnisdiensten. Anhand der Anforderungen muss also eine Entscheidung dahingehend getroffen werden, ob diese Leistungen durch eine eigene Infrastruktur oder durch Fremdanbieter in Anspruch genommen werden sollen. Die Er-

füllung dieser Anforderungen ist eine zwingende Voraussetzung, um die langfristige Vertrauenswürdigkeit des Archivierungs-Konzepts zu sichern.

Der Computer- und Medienservice der HU Berlin betreibt seit längerer Zeit eine eigene Zertifizierungsinstanz (HU-CA), die Zertifikate für Angehörige der Universität sowie für Server ausstellt. Hierbei handelt es sich um Zertifikate nach dem X509-Standard, die als Dateien gespeichert werden. Der Einsatz von Chipkarten zur Speicherung der Schlüssel ist in Planung. Obwohl die Nutzung der Zertifikate nicht auf bestimmte Anwendungen beschränkt ist, werden diese derzeit hauptsächlich für Zwecke der Authentisierung verwendet. Damit erstellte Signaturen würden einfache Signaturen im Sinne des Signaturgesetzes darstellen (siehe Abschnitt 3.2)

Die HU-CA ist ein hervorragendes Angebot für eine Reihe von Diensten, die innerhalb der Universität genutzt werden. Zur Anwendung im Rahmen des hier vorgestellten Konzepts für die Sicherung der Online-Publikationen auf dem Dokumentenserver wird jedoch die Nutzung der Dienste eines akkreditierten Trustcenters im Sinne des Signaturgesetzes empfohlen:

- Mit den zertifizierten Signaturschlüsseln können qualifizierte Signaturen nach Signaturgesetz erzeugt werden, d.h. dass im Rahmen eines möglichen Verwaltungsgerichtsverfahrens diese einen gesetzlich verordneten Anschein der Echtheit besitzen und somit problemlos als Beweismittel einsetzbar sind. So führt z.B. die Habilitationsordnung der Medizinischen Fakultät Charité in §17 aus: „Für alle verfahrensmäßigen wie die Leistung wertenden Entscheidungen im Habilitationsverfahren gelten die Vorschriften des Verwaltungsverfahrensgesetzes“ und weiter „Alle verfahrenserheblichen Mitteilungen an die Habilitandin oder den Habilitanden bedürfen der Schriftform, dies gilt insbesondere für belastende Entscheidungen und Fristenregelungen“. Zwar erscheint es derzeit noch etwas weit vorgegriffen, dass es zu Gerichtsverfahren im Zusammenhang mit elektronischen Publikationen kommen wird. Ohne eine genauere juristische Betrachtung durchzuführen, kann es aber eine Reihe von Fällen geben, in denen relevant ist, welche Dokumente wann vorgelegen haben. Beispielsweise könnte ein Promovend oder Habilitand abstreiten, ein bestimmtes Original eingereicht zu haben, oder bei urheberrechtlichen Streitigkeiten könnte nachgewiesen werden, dass ein Dokument zu einem bestimmten Zeitpunkt als Veröffentlichung bei der HU Berlin vorgelegen hat. Dies könnte zukünftig besonders dann interessant werden, wenn es um Publikationen geht, bei denen die Papierversi-

on nicht mehr zum Nachweis genutzt werden kann, z.B. bei zusätzlich veröffentlichten multimedialen Dokumenten, die auch Gegenstand der Begutachtung sind.

- Für eine vertrauenswürdige Erstellung der Signaturen ist eine Reihe von Voraussetzungen erforderlich, die vom akkreditieren Anbieter schon durch die gesetzliche Verpflichtung erfüllt und behördlich überprüft werden, wie z.B. die sichere Identifizierung der Antragsteller oder die Speicherung der Schlüssel auf Chipkarten, wodurch eine Nichtabstreitbarkeit der Signaturerzeugung erreicht wird. Wesentlich für das hier vorgestellte Konzept ist der Betrieb eines Zeitstempeldienstes und die langfristige Prüfbarkeit der Zertifikate, die bei einem akkreditierten Anbieter mindestens noch 30 Jahre nach Ablauf der Gültigkeit gewährleistet ist.
- Die Realisierung vieler der oben genannten technischen Konzepte ist bei einer eigenständigen Umsetzung sehr kosten- und personalintensiv. Deshalb ist es sinnvoller, für einen kleinen Anwendungsbereich mit besonderen Anforderungen ein externes Angebot in Anspruch zu nehmen, als das interne Angebot mit Funktionen aufzurüsten, die für einen Großteil der Anwendungen nicht relevant ist. So ist z.B. die sehr aufwändige Inbetriebnahme eines vertrauenswürdigen Zeitstempeldienstes für Zwecke der Verschlüsselung oder Authentisierung nicht zwingend erforderlich, für die langfristige Prüfbarkeit von Signaturen jedoch unerlässlich.

Ausgehend von den vorhergehenden Betrachtungen sollen deshalb qualifizierte Signaturen mit Anbieterakkreditierung eingesetzt werden. In Deutschland gibt es dafür eine Reihe von Anbietern. Folgende betreiben eine eigene Infrastruktur: Authentidate, Datev, D-Trust, Signtrust, TC Trustcenter und Telesec. Es gibt weitere so genannte „virtuelle Trustcenter“, die die Infrastruktur dieser Anbieter zum Aufbau eines eigenen Angebots nutzen, wie z.B. einige Notar- und Steuerkammern. Diese bieten ihre Dienstleistungen aber in der Regel nur Angehörigen bestimmter Berufsgruppen an.

Jeder Mitarbeiter der „Arbeitsgruppe Elektronisches Publizieren“, der berechtigt ist, am Archivserver zu arbeiten, erhält eine persönliche Chipkarte. Derzeit sind dies vier Personen. Bis auf Telesec und Signtrust sind keine Anbieter bekannt, die auch Zertifikate in diesem geringen Umfang ausstellen und keine Zugehörigkeit zu einem bestimmten Verband oder einer Berufsgruppe verlangen. Authentidate hat sich auf die Integration von Lösungen zur Nutzung von Zeitstempeldiensten und zum Scannen und nachträglichen Signieren von Dokumenten spezialisiert. D-Trust wendet sich mit seinem Angebot

insbesondere an kleine und mittelständische Firmen, wobei die Beantragung von Zertifikaten grundsätzlich über die zuständige IHK erfolgt. Die Datev hat das Angebot auf Mitglieder eingeschränkt, wie z.B. Steuerberater, die ihre Infrastruktur dort betreiben lassen. TC Trustcenter scheint trotz Akkreditierung zum jetzigen Zeitpunkt gar keine qualifizierten Zertifikate anzubieten. Zumindest ist auf den Webseiten keinerlei Information darüber zu finden; auch die angebotenen Root-Zertifikate sind selbst signiert und nicht von der RegTP ausgestellt.

Bei der Telesec kann der Antrag in jedem T-Punkt vorgenommen werden, eine Einschränkung auf besondere Standorte mit Business-Service oder auch ein Online-Antrag sind jedoch vorgesehen. Es können Hauptzertifikate und Attributzertifikate beantragt werden. Auf Wunsch gibt es auch ein Paket mit Chipkartenleser. Als Anwendung steht PKS-Crypt 1.3 für Windows und SecuBusiness 1.5 zur Verfügung. PKS Crypt erlaubt durch die Integration in den Windows Explorer alle elementaren Operationen über Dateien und basiert auf einer bestätigten Funktionsbibliothek, besitzt selbst jedoch keine Bestätigung der RegTP. Die Software SecuBusiness wird von einem Partner, der SecuOnline AG, entwickelt. Sie integriert sich u.a. auch in Winword und erlaubt eine einfache Erstellung von Signaturen inklusive der Visualisierung der zu signierenden Daten. Es liegt für dieses Produkt aber weder eine Bestätigung noch eine Herstellererklärung zum signaturgesetzkonformen Einsatz vor.

Die Kosten für das Zertifikat des Telesec belaufen sich für die Beantragung einmalig auf EUR 27,35. Die jährliche Gebühr beträgt EUR 49,83. Darin enthalten sind die Ausstellung eines Attributzertifikats sowie die unbegrenzte Nutzung von Verzeichnisdiensten und Zeitstempeldienst.

Signtrust bietet seit einiger Zeit wieder die Möglichkeit der Beantragung von qualifizierten Zertifikaten auch für Einzelpersonen. Nachdem Signtrust den Betrieb bereits einmal eingestellt hatte, wurde er einige Monate später aufgenommen. Die Angebote beschränkten sich dann aber auf Business-Kunden. Nun scheint man das Angebot wieder erweitert zu haben. Die Beantragung erfolgt online auf der Website von Signtrust. Dabei wird ein PDF-Dokument erstellt, das ausgedruckt und an Signtrust gesendet wird. Die Authentifizierung erfolgt über das PostIdent-Verfahren. Als Applikationen scheinen nur Mailkomponenten zur Verfügung zu stehen, diese besitzen jedoch eine Bestätigung der RegTP.

Die Kosten für das Zertifikat betragen im ersten Jahr und in den Folgejahren EUR 45,24 . Bei Nutzung von Attributen im Hauptzertifikat oder in separaten Attributzertifikaten verdoppelt sich der jährliche Betrag auf EUR 90,48.

Aus folgenden Gründen wird empfohlen, die Zertifikate weiterhin beim Anbieter Telesec zu beziehen:

- Es liegen bereits Erfahrungen bei der Nutzung des Telesec-Angebots, insbesondere der Anwendung PKS-Crypt, vor.
- Die Kosten liegen durch die zwingende Inanspruchnahme eines Attributzertifikats zur Selbstbeschränkung niedriger als bei Signtrust (Jahresgebühr für vier Mitarbeiter bei Telesec ca. EUR 199, bei Signtrust ca. EUR 361).
- Als Anwendung werden bei Signtrust derzeit nur Mailkomponenten angeboten. Für die Zwecke des Archivservers ist jedoch eine einfache Anwendung auf Dateiebene erforderlich und ausreichend. Ob die Signtrust-Komponenten dies implizit mit enthalten, konnte jedoch nicht geprüft werden.

4.3.4 Inhalt der Zertifikate

Ausgehend von der Analyse der Ist-Situation sind bei der zukünftigen Beantragung von Zertifikaten folgende zusätzliche Anforderungen zu erfüllen:

- Es ist auf geeignete Art und Weise deutlich zu machen, dass die Signaturen, die durch die autorisierten Mitarbeiter erstellt werden, in Vertretung eines Dritten, nämlich der juristischen Person der Humboldt-Universität zu Berlin, erfolgen. Dies ist erforderlich, da das Zertifikat grundsätzlich erst einmal an eine natürliche Person gebunden ist, die Signatur aber in der Rolle als Mitarbeiter der HU und nicht als Privatperson zu erfolgen hat. Daraus ergibt sich, dass die HU auch die Möglichkeit haben muss, ein Zertifikat eines Mitarbeiters ohne seine Mitwirkung zu sperren. Dies ist insbesondere dann erforderlich, wenn der Mitarbeiter die Universität verlässt oder aus anderen Gründen nicht mehr berechtigt ist, Signaturen für den vereinbarten Anwendungszweck zu erstellen.
  Diese Anforderung wird im Folgenden als *Vertretungsmacht* bezeichnet.

- Die Nutzung der Zertifikate ist in geeigneter Form auf die Signatur und Zeitstempelung von Dokumenten zu beschränken, die im Rahmen der Bearbeitung von elektronischen Publikationen gemäß den Leitlinien des Dokumentenservers der HU Berlin anfallen. Damit wird zunächst einmal verhindert, dass die ausgestellten Zertifikate durch die Mitarbeiter für Zwecke benutzt werden, für die sie möglicherweise keine Legitimation besitzen. Das ist besonders relevant, da ja die Nutzung der Zertifikate in Vertretung der Humboldt-Universität erfolgt.
  Diese Anforderung wird im Weiteren als *Selbstbeschränkung* bezeichnet.

Für die beiden formulierten Anforderungen werden in den kommenden Abschnitten verschiedene Lösungsvarianten vorgestellt, diskutiert und bewertet.

4.3.4.1 Vertretungsmacht

Das Signaturgesetz sieht diesen Anwendungsfall explizit vor und gibt den Nutzern die Möglichkeit, für diesen Zweck so genannte Attribute zu definieren. Diese Attribute können entweder direkt im Zertifikat oder als separates Attributzertifikat angegeben werden.

Die Nutzung eines Attributzertifikats hat einige Vorteile aufzuweisen. Durch die Trennung in zwei verschiedene Zertifikate kann der Zertifikateinhaber bei jedem Vorgang entscheiden, ob er die Signatur als Privatperson oder in Vertretung des Dritten vornimmt. Auch mehrere Vertretungen einer dritten Person über verschiedene Attributzertifikate sind möglich. Damit erhöht sich die Flexibilität des Einsatzes der Zertifikate. Vor der Beantragung eines Attributzertifikats zur Vertretung Dritter ist dessen Einwilligung einzuholen. Hierzu sieht das derzeitige Antragsverfahren der Telesec eine notarielle Bestätigung über ein gesondertes Formular vor. Diese Anforderung wird in Zukunft auf eine einfache schriftliche Bestätigung reduziert, so dass sich der Aufwand für die Beantragung des Attributzertifikats deutlich reduziert.

Die beantragten Zertifikate für die Mitarbeiter der „Arbeitsgruppe Elektronisches Publizieren“ sollen jedoch ausschließlich für die Signatur von elektronischen Dokumenten genutzt werden. Eine Nutzung als Privatperson ist nicht vorgesehen, die Nutzung als Mitarbeiter der HU zwingend. Dies lässt sich über ein optionales Attributzertifikat nicht erreichen.

Eine weitere Möglichkeit, die Vertretungsmacht abzubilden, besteht darin, diese in das Namensfeld des Zertifikats mit aufzunehmen, z.B. „Peter Müller, HU Berlin“. Damit kommt die Verbindung zur vertretenden Stelle deutlich zum Ausdruck, und auch hier wäre eine Bestätigung notwendig, dass diese Vertretung tatsächlich besteht.

Schließlich kommt noch die Verwendung eines Pseudonyms in Frage. Das Zertifikat wird weiterhin auf eine natürliche Person ausgestellt, die auch alle im Antrag geforderten Angaben machen muss. Allerdings erscheint im Zertifikat nur das Pseudonym, das max. 20 Zeichen lang sein darf. Die dahinter stehende Person darf durch das Trustcenter nur in besonderen Fällen, wie z.B. auf Anforderung von Strafverfolgungsbehörden, offen gelegt werden. Während in vertraglichen Beziehungen die Verwendung eines Pseudonyms eher hinderlich sein dürfte, erfüllt es hier genau den beabsichtigen Zweck. Nicht der Name des Mitarbeiters, der die Signatur zu einem elektronischen Dokument erstellt hat, ist bei einer Prüfung interessant, sondern nur die Tatsache, dass diese Signatur mit einem gültigen Zertifikat der „Arbeitsgruppe Elektronisches Publizieren“ erzeugt wurde. Durch Führung und optional sogar Veröffentlichung einer internen Dokumentation zu ausgestellten Zertifikaten kann die hinter dem Zertifikat stehende Person problemlos ermittelt werden.

Die Intention des Gesetzgebers zum Konstrukt des Pseudonyms war es, aus datenschutzrechtlichen Gründen den Nutzern auch die Möglichkeit zu geben, in bestimmten Anwendungsfällen ohne Erscheinen ihres Namens agieren zu können. Insofern wird das Pseudonym in diesem Zusammenhang etwas zweckentfremdet. Allerdings machen die Zertifizierungsdiensteanbieter selbst Gebrauch davon, wie man an den CA-Zertifikaten leicht sieht, z.B. „Telesec PKS SigG CA 1:PN“. Auch diese Zertifikate sind letztendlich auf eine konkrete Person ausgestellt, die jedoch im Zusammenhang mit einem CA-Zertifikat nicht relevant ist.

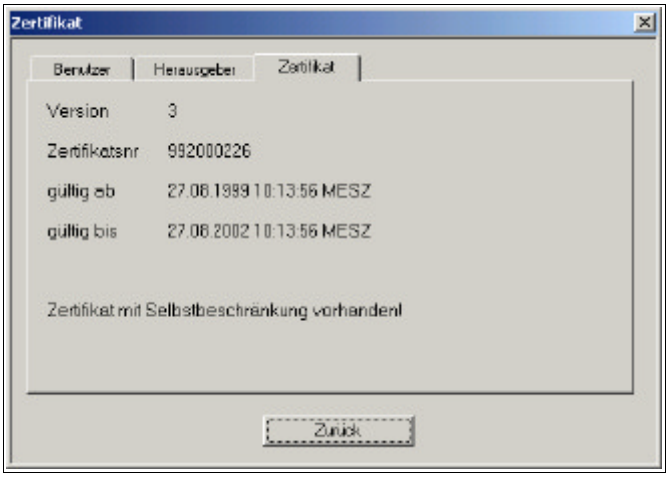
Auch Pseudonyme dürfen Hinweise auf eine Vertretung Dritter enthalten [SigG01 §5(3)]. Eine Bestätigung der vertretenden Stelle ist dem Zertifikatsantrag beizufügen.

Für die Zertifikate wird die Verwendung eines Pseudonyms empfohlen. Als Eintrag wird „EDOC CMS HU-BERLIN“ festgelegt. Eine Unterscheidung der Zertifikate bei gleichem Namen wird automatisch durch den Zertifizierungsdiensteanbieter vorgenommen, in dem er das Kürzel „PN“ zur Kennzeichnung des Namens als Pseudonym und eine Zahl

zur Unterscheidung hinzufügt. Die ersten beiden Einträge werden also „EDOC CMS HU-BERLIN:PN 1“ sowie „EDOC CMS HU-BERLIN:PN 2“ lauten.

4.3.4.2 Selbstbeschränkung

Auch für diesen Zweck sieht das Signaturgesetz die Möglichkeit der Nutzung von Attributen vor. Die Selbstbeschränkung kann dabei in das Hauptzertifikat aufgenommen werden, was bei der derzeitigen Zertifikatsstruktur der Telesec nicht vorgesehen ist, oder als separates Attributzertifikat ausgestellt werden. Im Unterschied zu einem Attributzertifikat zur Vertretung Dritter gibt es hier zumindest im Hauptzertifikat einen Hinweis, dass eine Selbstbeschränkung in Form eines Attributzertifikats existiert. Der Empfänger sollte eine Signatur dann ablehnen, wenn dieses Attributzertifikat nicht mitgeliefert wird.



Folgende Formulierung der Selbstbeschränkung wird vorgeschlagen:

Die Nutzung des Signaturschlüssels ist auf die Signatur von elektronischen Dokumenten beschränkt, die zur Veröffentlichung auf dem Dokumentenserver der HU Berlin bestimmt sind oder im Rahmen der durch die Leitlinien des Dokumentenservers der HU Berlin vorgegebenen Aufgaben verarbeitet werden.

Diese etwas kompliziert wirkende Formulierung schränkt den Handlungsspielraum so ein, dass alle regulären Aufgaben zur Archivierung der Dokumente erfüllt werden kön-

nen, aber keine weitergehenden Möglichkeiten zur Nutzung der Signatur vorhanden sind. So musste z.B. ausgeschlossen werden, dass die Signatur für Bestellungen, Konferenzanmeldungen o.ä. genutzt werden kann.

Es ist zu prüfen, ob im Zuge der Umstellung des Telesec-Trustcenters auf einen ISIS-MTT-kompatiblen Betrieb die Möglichkeit besteht, die Selbstbeschränkung direkt im Hauptzertifikat unterzubringen. Dies würde noch eine höhere Transparenz erzeugen und die Nutzung von Attributzertifikaten überflüssig machen.

4.3.5 Ausstellung der Zertifikate

Nachdem im vorangegangenen Abschnitt der ZDA Telesec für die Ausstellung der Zertifikate gewählt wurde, beschäftigt sich dieser Abschnitt konkret mit dem Verfahren der Beantragung der Zertifikate. Die Telesec bietet für diesen Zweck ein Paket mit allen notwendigen Formularen an, das bei den T-Punkten oder über den zentralen Service bezogen werden kann. Im Folgenden wird auf die Antragsversion vom Juli 2002 Bezug genommen. Das Paket besteht aus folgenden Formularen:

- *Antrag auf Teilnahme am Public Key Service gemäß den Anforderungen des deutschen Signaturgesetzes (PKS-SigG)*
  Dies ist das eigentliche Formular zur Beantragung der Zertifikate. Es fordert Angaben zur Person, zu Details der beantragten Zertifikate sowie zur Bezahlung der Leistungen aus diesem Vertrag. Das Formular findet sich im Anhang. Weiter unten in diesem Abschnitt folgen konkrete Hinweise zum Ausfüllen des Formulars.
- *Leitfaden zum Ausfüllen des Antrags auf Teilnahme am Public Key Service*
  Hier werden Hinweise zum Ausfüllen des Hauptformulars gegeben.
- *Informationen zur Teilnahme am Public Key Service*
  Diese Broschüre vermittelt grundsätzliche Informationen zu digitalen Signaturen, der praktischen Anwendung und den rechtlichen Grundlagen ihres Einsatzes.
- *Attribut-Zertifikat zur Selbstbeschränkung*
  Dieses Formular ist zu benutzen, wenn eine Beschränkung der Nutzung des Zertifikats, z.B. auf die ausschließliche Signatur von Dokumenten im Rahmen des elektronischen Publikationsprozesses, vorgesehen ist.

- *Attribut-Zertifikat zur berufsrechtlichen oder sonstigen Zulassung (Erlaubnis, Genehmigung, Konzession, Bewilligung o.ä.)*
  Mit diesem Formular können spezielle Berufsbezeichnungen, wie z.B. Facharzt für Allgemeinmedizin oder Notar, als Attribut-Zertifikat integriert werden. Da diese Ausstellung eine Prüfung der Zulässigkeit des Führens dieser Bezeichnung einschließt, muss der Antrag von einer für die Bezeichnung zuständigen Stelle (z.B. Bundesnotarkammer) bestätigt werden.
- *Attribut-Zertifikat zur Vertretungsmacht für einen Dritten (Teil I für den Antragsteller, Teil II für den Dritten)*
  Da Zertifikate immer nur für natürliche Personen ausgestellt werden, bei Signaturen jedoch häufig ein Agieren der Person in einer bestimmten Rolle einer juristischen Person erforderlich ist (z.B. Sachbearbeiter der Techniker Krankenkasse) kann hiermit wieder in einem zusätzlich ausgestellten Attribut-Zertifikat diese Vertretung eines Dritten nachgewiesen werden. Dazu ist eine Einverständniserklärung des Dritten erforderlich, und dieser erhält damit auch das Recht, das Zertifikat zu widerrufen.
- *Preisliste Public Key Service*

Wie bei der Durchsicht der vielen Formulare ersichtlich, ist eine Reihe von eigenhändigen Unterschriften notwendig, bevor endlich elektronisch signiert werden darf.

Die meisten Angaben des Antragsformulars sind selbsterklärend und vom Antragsteller persönlich auszufüllen. Da auch einige organisatorische Angaben verlangt werden, ist es sinnvoll, den Antrag gemeinsam mit der Verwaltungsleitung auszufüllen.

Unter Punkt 4 ist ein so genanntes Telepasswort anzugeben, das z.B. bei der telefonischen Sperrung eines Zertifikates abgefragt wird. Es ist bei der Verwaltungsleitung sicher zu hinterlegen. Die Zustellung der PKS-Karte kann per Post erfolgen. Das Zertifikat soll zum Abruf über das Zertifikatsverzeichnis freigegeben werden. Die Zahlungsweise für den PKS-Service ist durch die Verwaltungsleitung festzulegen, die Zahlung per Rechnung ist sicherlich die einfachste Variante. Der Antrag ist erst bei der Abgabe an der entsprechenden Registrierungsstelle zu unterschreiben. Es wird eine Kopie des Personalausweises erstellt und an das Trustcenter geschickt.

Für das Attributzertifikat zur Selbstbeschränkung ist der in diesem Kapitel vorgeschlagene Text einzutragen. Die Zustellung kann per E-Mail erfolgen, da das Zertifikat mit dem öffentlichen Schlüssel aus dem Hauptzertifikat verschlüsselt wird.

Das Pseudonym hat einen Bezug zu einer zu vertretenden dritten Person. Deshalb ist laut Signaturgesetz §5 (3) eine Einwilligung einzuholen. Derzeit gibt es bei der Telesec nur ein vorgegebenes Verfahren bei Einholung eines Attributzertifikats zur Vertretung Dritter. Die Einwilligung ist sogar notariell zu bestätigen. Es wird eine Vereinfachung durch das Trustcenter angestrebt, bei der eine schriftliche Bestätigung ausreicht. Das Verfahren ist jedoch noch nicht genau definiert und muss vor der Beantragung geklärt werden.

Abbildung 4.2 Telesec Chipkarte

Nach der Zusendung der Karte muss diese zunächst freigeschaltet werden. Das erfolgt über die Funktion „Karte freischalten“ der Anwendung PKS-Crypt, was zugleich auch eine Sicherheitsfunktion darstellt, da die Freischaltung nur einmal pro Karte erfolgen kann. Falls sie fehlschlägt, muss die Karte vorher manipuliert worden sein. Die Zertifikate können dann von der Karte in die Anwendung gelesen und auf Korrektheit geprüft werden.

Anschließend muss noch ein Formular über den Erhalt der Karte ausgefüllt und an die Telesec zurückgesendet werden. Erst danach wird das Zertifikat in das Zertifikatsverzeichnis aufgenommen und ist offiziell zur Nutzung freigegeben. Falls die zugesendete Karte eine Wiederausstellung für ein abgelaufenes Zertifikat sein sollte, wird das alte gesperrt.

4.3.6 Archivierungsstruktur

Im Folgenden wird eine Dateisystemstruktur für die Ablage der Dokument-Dateien entworfen, um einen effizienten Zugriff im Rahmen aller Archivierungsaufgaben zu ermöglichen. Dabei ist insbesondere zu berücksichtigen, dass sich Teile des Dokuments im Rahmen des Publikationsprozesses ändern können. Dies ist z.B. der Fall, wenn

- zusätzliche Konvertierungen in weitere Dateiformate durchgeführt werden,
- Änderungen an Metadaten erfolgen,
- im Rahmen der Langzeitsicherung der Dokumente alte Dateiformate in neue konvertiert werden.

Alle erfolgten Änderungen sind zu archivieren und die Dateien zu sichern. Damit nicht bei jeder Archivierung die gesamten Dateien separat gehalten werden müssen, werden nur die Unterschiede innerhalb der Verzeichnisstruktur gespeichert. Es wird ein Algorithmus definiert, mit dem neue Dokumente erkannt, geänderte aktualisiert und Löschungen vorgenommen werden können. Das Löschen eines Teildokuments ist ein eher seltener Fall und könnte z.B. dann erfolgen, wenn gegen das Datenschutzgesetz verstoßen wurde.

Die Ordnerstruktur wird durch eine dreistufige Hierarchie abgebildet. Auf der ersten Ebene werden Ordner mit dem URN des Dokuments angelegt. Auf der zweiten Ebene folgen Ordner mit Zahlen beginnend mit der Ziffer 1. Dadurch ergibt sich eine Chronologie, in der Änderungen am Dokument gespeichert werden können. Auf der dritten Ebene schließlich werden Ordner angelegt, um die Dateien entsprechend ihrer Zugehörigkeit zu den bereits weiter oben festgelegten Dokumentgruppen zu speichern. Die Dateien werden dabei trotz ihrer Zugehörigkeit zu mehreren Gruppen nur einmal innerhalb der Ordnerstruktur gespeichert. Auf dieser Ebene werden folgende Verzeichnisse angelegt:

- ORIGINAL: Für die Originaldateien aus dem Textverarbeitungssystem des Autors, die Abstract-Dateien, die Keyword-Dateien.
- PDF: Die vom Autor generierte PDF-Datei.
- SGML: Die durch die Konvertierung erzeugten SGML-Dateien gemäß der DiML mit der Dateiendung .did .

- HTML: Durch Konvertierung aus den SGML-Dateien gewonnene HTML-Version des Dokuments.
- BINARY: Alle zusätzlichen Teile des Dokuments, wie z.B. Bilder, Videos, Audios oder Programme. Dabei werden durch die Konvertierung nach SGML/HTML erzeugte Dateien im Unterordner CONV und bereits vorhandene Dateien im Unterordner ORIG abgelegt.
- METADATA: Eine XML-Datei mit den Metadaten aus der bibliografischen Erfassung des Dokuments.
- ARCHIVEDATA: Hier wird die erzeugte Archiv-Sicherungsdatei (siehe nächster Abschnitt) sowie die Signatur- und Zeitstempeldatei gespeichert.

Der Ordner mit der Nummer 1 wird die Dateien enthalten, die im Original vom Autor eingereicht werden. Der Ordner 2 wird im allgemeinen zusätzlich die konvertierte SGML- bzw. HTML-Version sowie die Metadaten aufnehmen. Ab Ordner 3 werden in der Regel Änderungen am Dokument abgelegt.

4.3.7 Entwurf der Archiv-Sicherungsdatei (ASD)

Es ist nicht praktikabel und notwendig, jede für die Archivierung gemäß Abschnitt 4.4.2 relevante Datei einzeln zu signieren und zu zeitstempeln. Vielmehr ist es ausreichend, eine Metadatei (Archiv-Sicherungsdatei) zu erzeugen, die eindeutige Referenzen auf die zugrunde liegenden Dateien enthält. Die eindeutige Referenz wird durch Bildung eines Hash-Wertes mit einem im Abschnitt „Hash-Verfahren“ beschriebenen und vom BSI empfohlenen kryptografischen Algorithmus erstellt. Zusätzlich wird dieses verwendete Verfahren innerhalb der Archiv-Sicherungsdatei dokumentiert. Zusammen mit weiteren Informationen, die in diesem Abschnitt noch beschrieben werden, wird dann nur diese Datei signiert und mit einem Zeitstempel versehen. Dies stellt keine Verringerung der Sicherheit des Verfahrens dar, da bei der Signatur einer einzelnen Datei auch nur der Hash-Wert verwendet wird. Durch die schon beschriebenen kryptografischen Eigenschaften von Hash-Verfahren ist die praktische Eindeutigkeit des Hash-Wertes zu einem Originaldokument gewährleistet. Bei der Prüfung der Integrität und Authentizität des Gesamtdokuments oder auch nur von Teilen ist diese für die Archiv-Sicherungsdatei vorzunehmen und ein Vergleich zwischen dem in der Datei gespei-

cherten Hash-Wert und einem gerade aus dem vorliegenden und zu prüfenden Dokument errechneten Wert durchzuführen. Stimmen die beiden Werte überein und wurde die Prüfung für die ASD erfolgreich durchgeführt, gilt die Integrität und Authentizität genauso für die zu prüfende Datei.

Die Definition der Archiv-Sicherungsdatei leistet aber noch mehr als eine Zusammenfassung mehrerer inhaltlich zusammengehörender Dateien eines Dokuments und eine Verringerung des Signaturaufwands. Vielmehr wird durch entsprechende Zusatzinformationen auch die Bedeutung der angebrachten Signatur bzw. des Zeitstempels definiert. Während das einfache Signieren und Zeitstempeln einer Datei zunächst einmal nichts weiter bedeutet, als dass eine bestimmte Bitfolge spätestens zu diesem Zeitpunkt dem Signierer vorlag, können aus der Archiv-Sicherungsdatei noch folgende Informationen bezogen werden:

- Alle einzelnen und durch ihren Hash-Wert und Namen vertretenen Dateien wurden vom Signierer mit einem zum zusätzlich definierten MIME-Type passenden Viewer in einer bestimmten Systemumgebung betrachtet und somit auf korrekte Darstellung und grobe Fehler geprüft. Selbstverständlich kann hierbei weder inhaltliche Richtigkeit garantiert werden noch jeder mögliche Darstellungsfehler ausgeschlossen werden. Geprüft werden kann aber beispielsweise (z.T. sicherlich auch nur stichprobenartig), ob die Seiten-Identität zwischen PDF- und HTML-Dokument gesichert ist oder ob grobe Darstellungsfehler vorhanden sind, die die Bedeutung des Textes beeinflussen können. Damit wird im Wesentlichen also das bereits beschriebene Präsentationsproblem adressiert. Es ist leicht zu ersehen, dass hier nur ansatzweise das in [Pordesch01] vorgeschlagene Verfahren der „Standardpräsentation“ umgesetzt wurde und die Vertrauenswürdigkeit von der Sorgfalt des Bearbeiters abhängt. Jedoch sichert es zumindest die korrekte Anzeigbarkeit unter den definierten Systemparametern und weiteren inhaltlichen Kriterien, die u.U. auf eine manuelle Kontrolle des Autors nach Konvertierung erweitert werden kann. Dies erscheint insbesondere unter dem Aspekt sinnvoll, dass naturgemäß Unterschiede im Layout zwischen der PDF-Version und der nach HTML konvertierten Version vorliegen.

  Die jeweils für den MIME-Type gültigen Systemparameter wie Hardware und Software werden in einer separaten Dokumentation erfasst. So kann unter Benutzung des Zeitstempels der ASD jederzeit geprüft werden, womit die relevante Datei auf

korrekte Darstellung geprüft wurde. Vorgaben zum Inhalt des Prüfverfahrens sind ebenfalls zu dokumentieren.

- Die einzelnen Dateien innerhalb der Archiv-Sicherungsdatei können Dateigruppen zugeordnet werden, um die Zugehörigkeit zu den jeweiligen Präsentationsformen darzustellen. Derzeit verwendete Gruppen sind z.B. 'PDF','SGML','HTML', 'Original','Metadaten'. Dabei kann eine Datei mehreren Gruppen zugeordnet werden, um Doppelerfassungen zu vermeiden, z.B. Bilder, die sowohl Bestandteil der SGML- als auch der HMTL-Version sind. Durch dieses Verfahren ist es sehr einfach möglich festzustellen, welche Dateien bei der Veröffentlichung der jeweiligen Präsentationsform genutzt werden, d.h. es ist möglich, jeweils sowohl für eine Gruppe als auch für das Gesamtdokument eine Vollständigkeitsinformation abzuleiten. Die Annahme und Konvertierung einer Dissertation verläuft üblicherweise in mehreren Stufen, so dass beim Hinzukommen von Dateien diese in einem weiteren Archivierungspaket einfach ergänzt werden oder die Zugehörigkeit zu einer Dateigruppe erweitert wird. Zum Beispiel gehört ein Softwareprogramm, das zu einer Arbeit abgeliefert wird, sicherlich zu allen vier Gruppen, während die separate Metadaten-Datei nur in die Gruppe 'Metadaten' einsortiert und derzeit in keiner anderen Publikationsform veröffentlicht wird.

- Zur Identifikation und Einordnung der Archiv-Sicherungsdatei werden zwei Merkmale genutzt. Zum einen wird schon frühzeitig für das Gesamtdokument ein Uniform Resource Name (URN) genutzt, der eine serverunabhängige Identifikation und Auffindbarkeit der elektronischen Version ermöglichen soll. Dieser wird in Form einer National Bibliographic Number (NBN) vergeben. Das Resolving der URN auf eine konkrete URL erfolgt auf einem Server der Deutschen Bibliothek. Informationen zur Verwendung innerhalb des CMS sind in [Dobratz03] beschrieben. Grundlagen zur Anwendung von URNs findet man ebenfalls auf dem Server der Deutschen Bibliothek [DDB03a]. Der URN bildet somit die Identifkation für das Gesamtdokument und eine Klammer um die einzelnen Dateien in der Archiv-Sicherungsdatei.
  Des Weiteren ist es notwendig, eine Chronologie zwischen mehreren ASDs herstellen zu können. ASDs ändern sich immer dann, wenn Dateien hinzukommen, wie z.B. bei einer zeitlich entkoppelten Konvertierung von PDF und HTML oder auch bei der Änderung von Dateien, z.B. von Metadaten-Einträgen. Die Reihenfolge wird durch eine Zahl beginnend mit 1 festgelegt, die mit dem Vorhandensein jeder neuen

Version erhöht wird. Weiterhin wird das Erstellungsdatum integriert. Die letzte Archiv-Sicherungsdatei kann dann leicht als aktuellste Datei oder aus den Logeinträgen des Workflow-Systems bestimmt werden. Die Zusammengehörigkeit von verschiedenen ASDs wird durch den URN definiert. Eine nachträgliche Änderung des URN zu einem Dokument ist in diesem Rahmen derzeit nicht vorgesehen.

Zusätzlich enthält eine ASD immer die Referenzen auf die vorhergehende ASD sowie die Signatur und den Zeitstempel. Damit wird eine Verkettung der ASDs und eine kontinuierliche kryptografische Sicherung der vorhergehenden Dateien erzielt, da diese bei der Neuerstellung eventuell mit neuen Algorithmen oder größeren Schlüssellängen referenziert werden und dadurch trotz Verlust der Sicherheitseignung ein Nachweis von Authentizität und Integrität vorheriger ASDs möglich ist.

- Um die Bedeutung der Signatur unter einer Archiv-Sicherungsdatei zu definieren, enthält diese einen Disclaimer, der Angaben zu ihrer Bedeutung enthält:

Dieses Dokument ist eine Archiv-Sicherungsdatei für elektronische Publikationen der HU Berlin.

Sie enthält Referenzen auf alle im Archiv aufbewahrten Dateien zu diesem Dokument.

Die Erstellung dieser Datei erfolgte gemäß den Richtlinien für die Archivierung und den Dokumentenserver der HU Berlin.

Die Hash-Werte der Dateien wurden innerhalb einer besonders gesicherten Systemumgebung mit einem vertrauenswürdigen Programm erstellt. Alle Dateien wurden mit einem zum MIME-Type passenden Viewer geprüft.

Für die Archiv-Sicherungsdatei wurde eine qualifizierte Signatur mit Anbieterakkreditierung der „Arbeitsgruppe Elektronisches Publizieren“ sowie ein Zeitstempel erzeugt.

Fragen zum Inhalt dieses Dokuments werden unter der angegebenen Kontaktadresse beantwortet.

Die technische Realisierung der Archiv-Sicherungsdatei erfolgt in Form einer XML-Datei mit einem im weiteren beschriebenen Schema. Dadurch kann die ASD mit einem beliebigen Text-Viewer betrachtet und der Inhalt intuitiv erfasst werden. Obwohl eine solche Datei im Wesentlichen auch manuell erstellt werden kann, ist die automatische Erzeugung im Rahmen des Workflows für elektronische Publikationen dringend zu empfehlen, da insbesondere die Konvertierung nach SGML bzw. HTML eine ganze Reihe Einzeldateien erzeugt.

4.3.7.1 Erstellung der Archiv-Sicherungsdatei

Der folgende Abschnitt beschreibt, wie die einzelnen Tags bei Erstellung der Archiv-Sicherungsdatei zu füllen sind und wie Änderungen an Dokumenten verarbeitet werden. Es wird dazu das XML-Schema aus Anhang B verwendet.

XML-Tag	**Beschreibung**
<archive>	Start-Tag für das gesamte Paket
<urn>	Bereits bei der Abgabe einer Publikation sollte aus dem Pool ein URN bestimmt werden, der ab diesem Zeitpunkt zur allgemeinen Identifizierung genutzt wird. Das Präfix des URN wird weder in der XML-Datei noch bei der Benennung der Archiv-Sicherungsdatei verwendet.
<counter>	Dieses Tag enthält eine Zahl beginnend mit 1 und stellt damit eine Chronologie zwischen den ASDs her. Die Zahl bezieht sich gleichzeitig auf das Verzeichnis der Archiv-Ordnerstruktur, die gerade bearbeitet wird.
<date>	Das Erstellungsdatum der Archiv-Sicherungsdatei wird im ISO 8601:2000 Format [ISO00a] eingetragen, z.B. 2003-06-25.
<contact>	Hier wird die jeweils aktuelle Anschrift der „Arbeitsgruppe Elektronisches Publizieren“, insbesondere die Email-Adresse eingetragen. Da die Archiv-Sicherungsdatei auch veröffentlicht werden kann, wird den Nutzern die Möglichkeit gegeben, bei eventuellen Fragen Kontakt aufzunehmen.

XML-Tag	Beschreibung
<documentType>	Dieses Tag stellt den Typ der Publikation dar. Derzeit ist einer der Werte 'Dissertation', 'Habilitation', 'Vorlesung' ,'Diplom / Magisterarbeit', 'Zeitschrift', 'Monographie', 'Sonstige'. Alternativ könnten auch die englischen Begriffe verwendet werden, um die Einheitlichkeit zu erhöhen.
<title>	Es wird der Titel der Publikation eingetragen.
<author>	Es werden die Autoren der Publikation eingetragen.
<file>	Start-Tag für jede Datei des Dokuments
<uri>	Referenz auf die Datei. Diese wird derzeit als relativer Pfad innerhalb der Ordnerstruktur des Dokuments unterhalb des URN angegeben, z.B. 1/Pdf/Mertens.pdf.
<DocGroup>	Das Tag enthält die Zuordnung der Datei zu einer der definierten Dateigruppen 'PDF', 'HTML', 'SGML', 'Original' oder 'Metadaten'. Eine Mehrfachzuordnung ist zulässig.
<MimeType>	Enthält den MIME-Type der referenzierten Datei. Dieser sollte bei der Implementation eines Tools zur Unterstützung der Erstellung der Archiv-Sicherungsdatei aus der Dateiendung generiert und dem Bearbeiter vorgeschlagen werden. Eine Liste der derzeit verwendeten Typen ist im XML-Schema als Restriction vorgegeben. Zu diesen existiert auch jeweils die dokumentierte Viewer-Software. Eine Erweiterung ist jedoch jederzeit möglich.
<DigestMethod>	Hier ist die Angabe zum für die Referenzierung der Dateien genutzten Hash-Algorithmus einzutragen. Dies erfolgt entsprechend der Empfehlung der W3C Recommendation zu XML-Signaturen [W3C02a]. Bei der Auswahl sollen die regelmäßigen Empfehlungen des BSI zu geeigneten Kryptoalgorithmen zugrunde gelegt werden. Der hier verwendete Algorithmus SHA-1 ist bis mindestens Ende 2008 als ausreichend sicher anzusehen und wird mit dem Eintrag http://www.w3.org/2000/09/xmldsig#sha1 referenziert.

XML-Tag	Beschreibung
<DigestValue>	Mit einem vertrauenswürdigen und dokumentierten Programm wird der Hash-Wert zur Datei berechnet und BASE64-kodiert eingetragen.
<Comment>	Dieses Feld wird mit den Gründen für die Erstellung der Archiv-Sicherungsdatei versehen, z.B. die erstmalige Erstellung, Konvertierung in ein neues Zielformat, Änderungen von Metadaten oder Löschen von Dateien.
<Disclaimer>	Das Feld enthält den Absatz zum Inhalt und zur Bedeutung der Archiv-Sicherungsdatei.

Die Angaben in den Tags <documentType>, <title>, <author> dienen nur der Verbesserung der Lesbarkeit und Erleichterung der Zuordnung der Archiv-Sicherungsdatei. Für die Zwecke der Archivierung ist die Angabe des URN sowie die Referenzen auf die Dateien ausreichend.

Bei Änderungen an der Publikation wird ein weiterer Ordner mit der festgelegen Struktur (und leeren Inhalten) angelegt, wobei der Ordner als Namen den letzten Wert von <counter>+1 erhält. Dann werden alle geänderten oder neuen Dateien in die entsprechenden Ordner kopiert. Anschließend wird eine neue Archiv-Sicherungsdatei *urn_<counter>+1.xml* erstellt, die die gesamte Arbeit vollständig erfasst. Dabei wird wie folgt vorgegangen:

1. Es wird ein Index aller Dateien der letzten Archiv-Sicherungsdatei *urn_<counter>.xml* angelegt.
2. Für jede Datei, die sich in der neuen Ordnerstruktur *<counter>+1/* befindet, wird geprüft, ob sie im Index vorhanden ist. Wenn ja, stellt dies eine Änderung der Datei dar. In der ASD wird ein Eintrag für diese Datei mit einer Referenz auf den Ordner *<counter>+1/* erzeugt.
3. Für jede andere Datei im Index wird geprüft, ob sie sich noch an der angegebenen Stelle befindet. Wenn ja, dann hat sich an der Datei nichts geändert und sie ist weiterhin vorhanden. Es wird eine Referenz auf den Ordner erzeugt, diese ist identisch

mit der in der letzten ASD erzeugten. Falls die Datei nicht mehr gefunden wird, ist der seltene Fall einer Löschung eingetreten. Es wird keine Referenz in der neuen ASD erzeugt, es wird jedoch zwingend ein Kommentar eingefügt, der den Grund für die Löschung enthält.

4. Schließlich werden für alle Dateien, die sich in der Ordnerstruktur <counter>+1/ befinden und nicht in der aktuellen ASD vorhanden sind, neue Referenzeinträge auf die neue Struktur erzeugt.

Im Regelfall werden zunächst zwei oder drei Archiv-Sicherungsdateien erzeugt, die erste bei Abgabe des Dokuments durch den Autor, die weiteren bei Konvertierung nach PDF und SGML/HTML oder bei Hinzufügung der bibliothekarisch erzeugten Metadaten. In größeren zeitlichen Abständen wird gemäß der Verpflichtung zur Langzeitarchivierung eine Konvertierung bestimmter Dateien in andere Formate erfolgen.

Aufgrund dessen, dass nur die Änderungen abgelegt werden, entstehen in der ASD zwar Einträge mit Referenzen auf unterschiedliche Ordnerstrukturen unterhalb des Hauptverzeichnisses des Dokuments, allerdings wird dadurch weitestgehend eine Redundanz von Dateien vermieden. Bei den erzeugten Datenmengen und der Anzahl der publizierten Dokumente wird so eine erhebliche Speicherplatzmenge eingespart. Es ergibt sich von selbst, dass jeweils der gesamte Dokumentenordner durch ein Backup gesichert werden muss, da sich zu prüfende Dateien in allen Unterverzeichnissen befinden können.

Die Löschung von Dateien wird nur im Einzelfall vorkommen, wenn es sich im Nachhinein aus datenschutzrechtlichen oder urheberrechtlichen Aspekten ergibt oder mit dem Inhalt gegen andere Gesetze oder Regelungen verstoßen wird. Möglich wäre z.B., dass der Autor Bilder in seiner Arbeit verwendet hat, die Rechte anderer verletzen. Ältere Archiv-Sicherungsdateien und die zugeordneten Zeitstempel und Signaturen, die sich auf einen Dokumentenstatus vor der Löschung der Datei beziehen, werden trotzdem nicht ungültig, da nur zu bestimmten Referenzeinträgen in der Archivierungsstruktur keine Datei mehr gefunden werden kann. Ein Blick in eine der nachfolgenden ASD enthält dann im Kommentarfeld auch den Grund für die Löschung.

4.3.7.2 Beispiel für eine Archiv-Sicherungsdatei

Dieser Abschnitt beschreibt anhand einer real existierenden Dissertation den Ablauf für die Erstellung der Archiv-Sicherungsdateien sowie das Vorgehen bei Änderung, Neuerfassung und Löschung von Dateien. Es werden die zu erzeugenden Ordnerstrukturen und die wesentlichen Teile der jeweils dazu generierten ASDs dargestellt.

Das Beispiel umfasst die Dissertation von Frank Mertens aus dem Jahre 2000 an der Charité. Folgendes Szenario wird abgehandelt:

1. Abgabe der Originaldateien der Dissertation, der PDF-Version und der Abstract-und Keyword-Dateien.
2. Konvertierung der Arbeit nach SGML und HTML. Hinzufügen der bibliothekarischen Metadaten.
3. Löschung des hinzugefügten Programms aus urheberrechtlichen Gründen. Aktualisierung der Metadaten-Datei.

Da bisher noch keine reguläre URN-Vergabe erfolgt, wird ein fiktiver URN gewählt: 089-1234567890.

Der Ordner mit dem URN und der erste Unterordner werden angelegt:

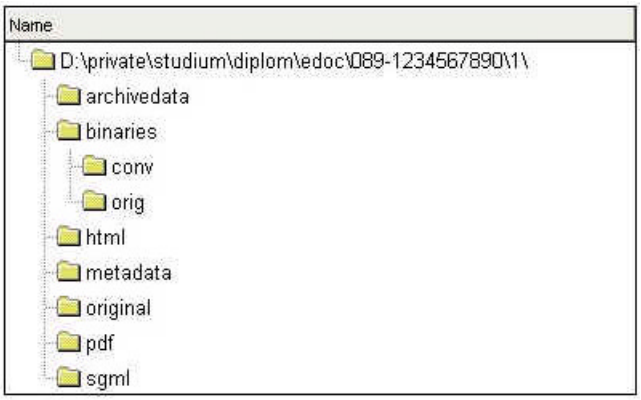


Abbildung 4.3 Ordnerstruktur Archiv

Anschließend werden die für Schritt 1 genannten Dateien in diese Struktur kopiert. Aus Gründen der Darstellbarkeit wurden nicht alle der zur Arbeit gehörenden Bilder berücksichtigt.

Abbildung 4.4 Abgabedateien des Autors

An dieser Stelle wird die erste Archiv-Sicherungsdatei erzeugt, mit der belegt werden kann, wann der Autor die Arbeit abgegeben hat.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!-- edited with XMLSPY v5 rel. 2 U (http://www.xmlspy.com) by Daniel Ohst -->
<archive>
    <urn>urn:nbn:de:gbv:089-1234567890</urn>
    <counter>1</counter>
    <creation_date>22.01.2000</creation_date>
    <contact>
    Arbeitsgruppe Elektronisches Publizieren
    Humboldt-Universität zu Berlin
    Erwin Schrödinger-Zentrum
    Rudower Chaussee 26
    12489 Berlin
    edoc@cms.hu-berlin.de
    </contact>
    <documentType>Dissertation</documentType>
    <title>Entwicklung eines Computerprogramms zur Durchführung elektronischer Setups</title>
    <author>Mertens, Frank</author>
    <file>
        <uri>1/binaries/orig/bild1.jpg</uri>
        <MimeType>image/jpeg</MimeType>
        <DocGroup>ORIGINAL</DocGroup>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>oZ4OBEtQtKc2hR7gatQQBglfdOk=</DigestValue>
    </file>
    <file>
        <uri>1/binaries/orig/bild13.jpg</uri>
        <MimeType>image/jpeg</MimeType>
```

```
        <DocGroup>ORIGINAL</DocGroup>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>Z8MIGj+WPfqojmbM9XgDjImZCIY=</DigestValue>
    </file>
    <file>
        <uri>1/binaries/orig/bild21.jpg</uri>
        <MimeType>image/jpeg</MimeType>
        <DocGroup>ORIGINAL</DocGroup>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>nuXMGeKVfXGTY3AcDaOYubUuxCE=</DigestValue>
    </file>
    <file>
        <uri>1/binaries/orig/virtarj.exe</uri>
        <MimeType>application/octet-stream</MimeType>
        <DocGroup>ORIGINAL</DocGroup>
        <DocGroup>PDF</DocGroup>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>slBdNRONBflhVoDMja9Z8eRNP+Q=</DigestValue>
    </file>
    <file>
        <uri>1/original/abstr_de.doc</uri>
        <MimeType>application/ms-word</MimeType>
        <DocGroup>ORIGINAL</DocGroup>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>uHX6jlIMM36Vm5AR7B9QXHSNQxk=</DigestValue>
    </file>
    <file>
        <uri>1/original/abstr_en.doc</uri>
        <MimeType>application/ms-word</MimeType>
        <DocGroup>ORIGINAL</DocGroup>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>SMC0gghhPa6TCeATXQ8GfimPjqQ=</DigestValue>
    </file>
    <file>
        <uri>1/original/dok_vkn.doc</uri>
        <MimeType>application/ms-word</MimeType>
        <DocGroup>ORIGINAL</DocGroup>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>LrqGTJ2VEvgooBsZUWh8JCHWWWw=</DigestValue>
    </file>
    <file>
        <uri>1/original/eidessta.doc</uri>
        <MimeType>application/ms-word</MimeType>
        <DocGroup>ORIGINAL</DocGroup>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>noxnLrN63tbfw4dk9Nj1d0rcqIU=</DigestValue>
    </file>
    <file>
        <uri>1/pdf/mertens.pdf</uri>
        <MimeType>application/pdf</MimeType>
        <DocGroup>PDF</DocGroup>
        <DigestValue>mTjVYmwfASSSTa8QmdqqLSwiQCE=</DigestValue>
    </file>
    <Comment>Der Autor hat das Dokument am 22.01.2000 eingereicht und damit die Publikationspflicht in Bezug auf die elektronische Fassung erfüllt.</Comment>
    <Disclaimer>Dieses Dokument  ist eine Archiv-Sicherungsdatei für elektronische Publikationen der HU Berlin.
    Sie enthält Referenzen auf alle im Archiv aufbewahrten Dateien zu diesem Dokument.
    Die Erstellung dieser Datei erfolgte gemäß den Richtlinien für die Archivierung und den Dokumentenserver der HU Berlin.
    Die Hash-Werte der Dateien wurden innerhalb einer besonders gesicherten Systemumgebung mit einem vertrauenswürdigen Programm erstellt. Alle Dateien wurden mit einem zum MIME-Type passenden Viewer geprüft.
    Für die Archiv-Sicherungsdatei wurde eine qualifizierte Signatur mit Anbieterakkreditierung der „Arbeitsgruppe Elektronisches Publizieren“ sowie ein Zeitstempel erzeugt.
    Fragen zum Inhalt dieses Dokuments werden unter der angegebenen Kontaktadresse beantwortet.</Disclaimer>
</archive>
```

In Schritt 2 erfolgt die Konvertierung der Dissertation nach SGML und HTML. Außerdem wird aus dem Bibliothekssystem ein Extrakt der erfassten Metadaten in Form einer XML-Datei bereitgestellt. Es ergibt sich (unter Einbeziehung der ersten ASD mit ihrer Signatur und dem Zeitstempel) folgende Dateistruktur:

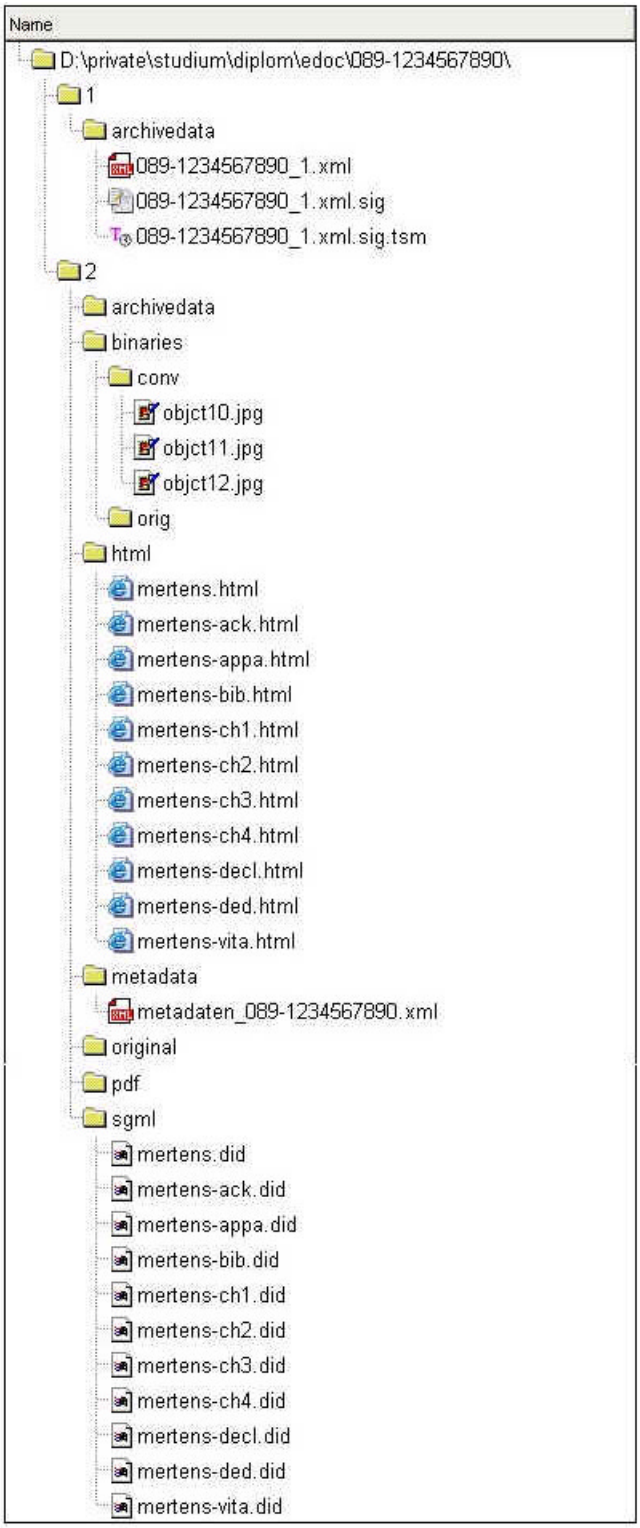


Abbildung 4.5 Konvertierung SGML/HTML

Da in diesem Schritt nur Dateien hinzugekommen sind, besteht die neue Archiv-Sicherungsdatei aus den Referenzen auf die Dateien aus dem Ordner 1/ sowie aus dem Ordner 2/.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!-- edited with XMLSPY v5 rel. 2 U (http://www.xmlspy.com) by Daniel Ohst-->
<archive>
	<urn>urn:nbn:de:gbv:089-1234567890</urn>
	<counter>2</counter>
	<creation_date>23.02.2000</creation_date>
	<contact>
	Arbeitsgruppe Elektronisches Publizieren
	Humboldt-Universität zu Berlin
	Erwin Schrödinger-Zentrum
	Rudower Chaussee 26
	12489 Berlin
	edoc@cms.hu-berlin.de
	</contact>
	<documentType>Dissertation</documentType>
	<title>Entwicklung eines Computerprogramms zur Durchführung elektronischer Setups</title>
	<author>Mertens, Frank</author>

<file><uri>1/binaries/orig/bild1.jpg</uri><MimeType>image/jpeg</MimeType><DocGroup>ORIGINAL</DocGroup>
	<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>oZ4OBEtQtKc2hR7gatQQBglfdOk=</DigestValue></file>


<file><uri>1/binaries/orig/bild13.jpg</uri><MimeType>image/jpeg</MimeType><DocGroup>ORIGINAL</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>Z8MIGj+WPfqojmbM9XgDjImZCIY=</DigestValue></file>


<file><uri>1/binaries/orig/bild21.jpg</uri><MimeType>image/jpeg</MimeType><DocGroup>ORIGINAL</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>nuXMGeKVfXGTY3AcDaOYubUuxCE=</DigestValue></file>

<file><uri>1/binaries/orig/virtarj.exe</uri><MimeType>application/octet-stream</MimeType>
<DocGroup>ORIGINAL</DocGroup><DocGroup>PDF</DocGroup>
<DocGroup>SGML</DocGroup><DocGroup>HTML</DocGroup>
 <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>slBdNRONBfIhVoDMja9Z8eRNP+Q=</DigestValue></file>

<file><uri>1/original/abstr_de.doc</uri><MimeType>application/ms-word</MimeType>
<DocGroup>ORIGINAL</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>uHX6jlMM36Vm5AR7B9QXHSNQxk=</DigestValue></file>

<file><uri>1/original/abstr_en.doc</uri><MimeType>application/ms-word</MimeType>
<DocGroup>ORIGINAL</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>SMC0gghhPa6TCeATXQ8GfimPjqQ=</DigestValue></file>

<file><uri>1/original/dok_vkn.doc</uri><MimeType>application/ms-word</MimeType>
<DocGroup>ORIGINAL</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>LrqGTJ2VEvgooBsZUWh8JCHWWWw=</DigestValue></file>

<file><uri>1/original/eidessta.doc</uri><MimeType>application/ms-word</MimeType>
<DocGroup>ORIGINAL</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>noxnLrN63tbfw4dk9Nj1d0rcqIU=</DigestValue></file>

<file><uri>1/pdf/mertens.pdf</uri><MimeType>application/pdf</MimeType><DocGroup>PDF</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>mTjVYmwfASSSTa8QmdqqLSwiQCE=</DigestValue></file>
```

<file><uri>2/binaries/conv/objct10.jpg</uri><MimeType>image/jpeg</MimeType><DocGroup>HTML</DocGroup>
<DocGroup>SGML</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>Hna37U0EIwwa0Dwu5U2b6y1CNnE=</DigestValue></file>

<file><uri>2/binaries/conv/objct11.jpg</uri><MimeType>image/jpeg</MimeType><DocGroup>HTML</DocGroup>
<DocGroup>SGML</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>yuIU16oI9FxpnADhe/grnc1Zrl8=</DigestValue></file>

<file><uri>2/binaries/conv/objct12.jpg</uri><MimeType>image/jpeg</MimeType><DocGroup>HTML</DocGroup>
<DocGroup>SGML</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>PLdC6f9KKVyVVfrFxn77lV2dwR8=</DigestValue></file>

<file><uri>2/html/mertens.html</uri><MimeType>image/html</MimeType><DocGroup>HTML</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>2Fb6sBmGhJ8HLrFNt5gb0maJtzk=</DigestValue></file>

<file><uri>2/html/mertens-ack.html</uri><MimeType>image/html</MimeType><DocGroup>HTML</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>EdgSAWqfLb3zrPc5BZ9niTL1wWY=</DigestValue></file>

<file><uri>2/html/mertens-appa.html</uri><MimeType>image/html</MimeType><DocGroup>HTML</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>E+pWKXRPhJ9heZ0tIWHPWc714/A=</DigestValue></file>

<file><uri>2/html/mertens-bib.html</uri><MimeType>image/html</MimeType><DocGroup>HTML</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>volacuZ1UVNqimClY6OVvCAyRCg=</DigestValue></file>

<file><uri>2/html/mertens-ch1.html</uri><MimeType>image/html</MimeType><DocGroup>HTML</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>p1EKPDwjGOocV8lyL9bl+Xi8je0=</DigestValue></file>

<file><uri>2/html/mertens-ch2.html</uri><MimeType>image/html</MimeType><DocGroup>HTML</DocGroup>
<DigestValue>Hi5ZqhKdzuAsesWn36D7fOXrhT4=</DigestValue></file>

<file><uri>2/html/mertens-ch3.html</uri><MimeType>image/html</MimeType><DocGroup>HTML</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>eSePwj0vlPEDG3kgCOC+izf6aVs=</DigestValue></file>

<file><uri>2/html/mertens-ch4.html</uri><MimeType>image/html</MimeType><DocGroup>HTML</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>2EelyKBoKFWVYqYPJmpvYkgQ3ek=</DigestValue></file>

<file><uri>2/html/mertens-decl.html</uri><MimeType>image/html</MimeType><DocGroup>HTML</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>/EHpFhsIayS0nY0PBtzG24PIYUY=</DigestValue></file>

<file><uri>2/html/mertens-ded.html</uri><MimeType>image/html</MimeType><DocGroup>HTML</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>RIFJjsY53smCC80GH9WaNWUUYTM=</DigestValue></file>

<file><uri>2/html/mertens-vita.html</uri><MimeType>image/html</MimeType><DocGroup>HTML</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>c/SBhHdq2byu01V0RHkCy8imRIg=</DigestValue></file>

<file><uri>2/metadata/metadaten_089-1234567890.xml</uri><MimeType>text/xml</MimeType>
<DocGroup>METADATA</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>jmcOqN0/j4decmh/QtaA6QZUULc=</DigestValue></file>

<file><uri>2/sgml/mertens.did</uri><MimeType>text/sgml</MimeType><DocGroup>SGML</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>oHsAW1XIBmL+JdV9flx7SKR5PHk=</DigestValue></file>

<file><uri>2/sgml/mertens-ack.did</uri><MimeType>text/sgml</MimeType><DocGroup>SGML</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>vcRQELTAjOKRuOIRcmEY18iyVGQ=</DigestValue></file>

<file><uri>2/sgml/mertens-appa.did</uri><MimeType>text/sgml</MimeType><DocGroup>SGML</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>vLAsIh9jtaZdaVWW93s4IWRxSC4=</DigestValue></file>

<file><uri>2/sgml/mertens-bib.did</uri><MimeType>text/sgml</MimeType><DocGroup>SGML</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>HMgmTWDJHQVQHpSzAKAhSwZI54k=</DigestValue></file>

<file><uri>2/sgml/mertens-ch1.did</uri><MimeType>text/sgml</MimeType><DocGroup>SGML</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>GiUe9yRlTGZ3NzW9zFk0ByVZq7U=</DigestValue></file>

<file><uri>2/sgml/mertens-ch2.did</uri><MimeType>text/sgml</MimeType><DocGroup>SGML</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>filrd2tmPKM05dpYyrKqAdVrvvk=</DigestValue></file>

<file><uri>2/sgml/mertens-ch3.did</uri><MimeType>text/sgml</MimeType><DocGroup>SGML</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>Rs6qkkcocnalld0ayMZ2BPJcSq4=</DigestValue></file>

<file><uri>2/sgml/mertens-ch4.did</uri><MimeType>text/sgml</MimeType><DocGroup>SGML</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>bKR6+yqAaWCYUxrUboXTDgmvsNw=</DigestValue></file>

<file><uri>2/sgml/mertens-decl.did</uri><MimeType>text/sgml</MimeType><DocGroup>SGML</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>fbyJDjK/RHzRumx1VJmc6ra0oi0=</DigestValue></file>

<file><uri>2/sgml/mertens-ded.did</uri><MimeType>text/sgml</MimeType><DocGroup>SGML</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>LDT5yxLP/GAFkGO4i3FI6dbi1h4=</DigestValue></file>

<file><uri>2/sgml/mertens-vita.did</uri><MimeType>text/sgml</MimeType><DocGroup>SGML</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>cYvhB+057fedMmMhXzsTGivaJQs=</DigestValue></file>

<file><uri>1/archivedata/089-1234567890_1.xml</uri>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>WeC3UX4Xfy6sTPHh4svDYVUjhVw=</DigestValue></file>

<file><uri>1/archivedata/089-1234567890_1.xml.sig</uri>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>dgqVqE0mw0ukkHc1mXAUbD9R/YU=</DigestValue></file>

<file><uri>1/archivedata/089-1234567890_1.xml.sig.tsm</uri>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>ZSWoYy56uFsWUwU/yQWMipT08l0=</DigestValue></file>

<Comment/>
<Disclaimer>Dieses Dokument ist eine Archiv-Sicherungsdatei für elektronische Publikationen der HU Berlin.
Sie enthält Referenzen auf alle im Archiv aufbewahrten Dateien zu diesem Dokument.
Die Erstellung dieser Datei erfolgte gemäß den Richtlinien für die Archivierung und den Dokumentenserver der HU Berlin.
Die Hash-Werte der Dateien wurden innerhalb einer besonders gesicherten Systemumgebung mit einem vertrauenswürdigen Programm erstellt. Alle Dateien wurden mit einem zum MIME-Type passenden Viewer geprüft.
Für die Archiv-Sicherungsdatei wurde eine qualifizierte Signatur mit Anbieterakkreditierung der „Arbeitsgruppe Elektronisches Publizieren“ sowie ein Zeitstempel erzeugt.
Fragen zum Inhalt dieses Dokuments werden unter der angegebene Kontaktadresse beantwortet.</Disclaimer>
</archive>

Im dritten und letzten Schritt wird das Programm virtarj.exe aus dem Ordner 1/binaries/orig gelöscht, was in der neuen Archiv-Sicherungsdatei im Kommentar vermerkt wird. Des Weiteren wird die Metadaten-Datei erneuert. Die neue Dateistruktur sieht wie folgt aus:

Abbildung 4.6 Änderung Metadaten

Aus Platzgründen werden hier nur die Änderungen an der ASD aufgeführt, die sich im Gegensatz zur Version 2 geändert haben:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!-- edited with XMLSPY v5 rel. 2 U (http://www.xmlspy.com) by Daniel Ohst-->
<archive>
	<urn>urn:nbn:de:gbv:089-1234567890</urn>
	<counter>3</counter>
	<creation_date>14.05.2001</creation_date>
	<contact>
	Arbeitsgruppe Elektronisches Publizieren
	Humboldt-Universität zu Berlin
	Erwin Schrödinger-Zentrum
	Rudower Chaussee 26
	12489 Berlin
	edoc@cms.hu-berlin.de
	</contact>
	<documentType>Dissertation</documentType>
	<title>Entwicklung eines Computerprogramms zur Durchführung elektronischer Setups</title>
	<author>Martens, Frank</author>

...
```

```
<file><uri>3/metadata/metadaten_089-1234567890.xml</uri><MimeType>text/xml</MimeType>
<DocGroup>METADATA</DocGroup>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>xCbWZWGhc+G5qYsoTDtDEo7qjLk=</DigestValue></file>

<file><uri>1/archivedata/089-1234567890_2.xml</uri>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>dLY5zdFQF7q7f0V0myxwikEVWUQ=</DigestValue></file>

<file><uri>2/archivedata/089-1234567890_2.xml.sig</uri>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>dgqVqE0mw0ukkHc1mXAUbD9R/YU=</DigestValue></file>

<file><uri>2/archivedata/089-1234567890_2.xml.sig.tsm</uri>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>ZSWoYy56uFsWUwU/yQWMipT08l0=</DigestValue></file>
...

<comment>Die Datei 1/binaries/orig/virtarj.exe wurde aus urheberrechtlichen Gründen gelöscht.</comment>

...
```

4.3.8 Technische Signaturumgebung

Alle Funktionen, die im Zusammenhang mit der Archivierung der Dokumente stehen, werden auf einem speziell zu sichernden System, dem Archivserver ausgeführt. Er erfüllt im Einzelnen folgende Aufgaben:

- Speicherung aller auf dem Dokumentenserver publizierten Dokumente in der beschriebenen Ordnerstruktur
- Erzeugung der Archiv-Sicherungsdateien
- Erstellung der Signaturen und Zeitstempel für die ASDs
- Initiierung der eigentlichen Archivierung auf dem zentralen Backup-System der HU

Als Ansatz für die Konfiguration des Archiv-Server kann das Dokument „Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten“ der RegTP [RegTP02a] dienen. Dort werden Anforderungen an die Sicherheit von Signaturanwendungskomponenten sowie die Einsatzumgebungen formuliert. Es werden drei Umgebungen dargestellt:

- Ungeschützter Einsatzbereich mit ungesicherter Anbindung an das Internet und ohne signaturspezifische Sicherheitsvorkehrungen in der Einsatzumgebung (gegen Bedrohungen über Internet/Intranet und manuellen Zugriff Unbefugter/Datenaustausch per Datenträger).

- Geschützter Einsatzbereich mit Sicherheitsvorkehrungen, die eine hohe Sicherheit gegenüber potentiellen Angriffen über das Internet, ein angeschlossenes Intranet, einen manuellen Zugriff Unbefugter und Datenaustausch per Datenträger gewährleisten.
- Isolierter Einsatzbereich mit folgendem Schutz gegen potentielle Bedrohungen: Es erfolgt zu keinem Zeitpunkt eine Anbindung an ein Kommunikationsnetz, und in der Einsatzumgebung sind Sicherheitsvorkehrungen vorhanden, die potentielle Angriffe über manuellen Zugriff Unbefugter/Datenaustausch per Datenträger mit hoher Sicherheit abwehren.

Dabei werden die erste und die letzte Lösung sinnvollerweise als Sonderlösung und der geschützte Einsatzbereich als Regellösung betrachtet. Für den Archivserver ergibt sich schon automatisch, dass eine zumindest temporäre Anbindung an das Intranet (Übertragung der Dokumente von den Mitarbeiter-PCs auf den Archivserver, Zugriff auf das zentrale Backup-System) sowie das Internet (Herstellen der Verbindung zum Trustcenter für Zertifikatsprüfung und Zeitstempeldienst) erforderlich ist. Das Dokument schlägt weiterhin allgemeine Maßnahmen gegen die einzelnen Bedrohungsszenarien vor:

Risiko	**Sicherheitsvorkehrungen**
Angriff aus dem Internet	Hohe Sicherheit durch Abschottung
Angriff über das Intranet	IT-Plattform, Signaturanwendungskomponente
Angriff über manuellen Zugriff Unbefugter / Datenaustausch	Einsatzumgebung, IT-Plattform, Signaturanwendungskomponente
Fehler/Manipulation bei Installation, Betrieb / Nutzung, Wartung / Reparatur	Qualifiziertes / vertrauenswürdiges Personal, administrative Sicherheitsmaßnahmen

Es werden folgende Maßnahmen zur Erfüllung der Sicherheitsanforderungen vorgeschlagen:

- Der Archivserver wird im Recherraum des CMS aufgestellt. Damit wird ein hoher Zutrittsschutz erreicht.
- Es wird ein W2K-System mit allen derzeit empfohlenen Service Packs und Hotfixes installiert. Die Installationsdateien sind aus einer vertrauenswürdigen Quelle zu beziehen, z.B. von den Original-CDs aus dem MS Select-Vertrag.
- Der Archivserver wird nur dann eingeschaltet, wenn damit konkret gearbeitet wird. Wenn der Server ausgeschaltet ist, ist das Netzwerk-Kabel zu ziehen, um z.B. Angriffen über Wake-on-LAN zu entgehen.
- Zur weiteren Erhöhung des Zugangsschutzes sollte ein Festplattenverschlüsselungstool eingesetzt werden, wie z.B. Utimaco Safeguard. Die Zugangsdaten werden dabei sicher hinterlegt und ein unberechtigter Zugriff auf den Server deutlich erschwert.
- Der interne Zugriff auf die zu archivierenden Dateien soll über ein Transferlaufwerk eines dedizierten Fileservers erfolgen. Ein direkter Zugriff vom Archivserver auf Mitarbeiter-Rechner ist nicht zulässig.
- Zur Absicherung des Rechners gegenüber dem Internet und Intranet ist eine Firewall zu installieren, die nur den absolut notwendigen Datenverkehr zulässt. Die Verbindung zum Internet ist auf die benötigten Server des Trustcenters zu beschränken. Die Verbindung ins Intranet darf nur zum Transferserver und zum zentralen Backup-System zugelassen werden.
- Es ist ein vertrauenswürdiger Virenscanner zu installieren und regelmäßig mit den aktuellen Virensignaturen zu aktualisieren.
- Es ist ein nach den Anforderungen von Signaturgesetz bzw. Signaturverordnung geprüfter und bestätigter Chipkartenleser einzusetzen. Die bestätigten Produkte können auf der Website der RegTP abgerufen werden [RegTP03a].
- Es ist eine bestätigte und geprüfte Signaturanwendungskomponente einzusetzen. Derzeit ist problematisch, dass lediglich die Funktionsbibliothek, auf der PKS-Crypt basiert, eine Bestätigung besitzt, aber nicht das Produkt selbst. Es kann nur auf eine

Herstellererklärung auf der Website von Telesec verwiesen werden. Dies beeinträchtigt nicht die ordnungsgemäße Erstellung und Prüfung von Signaturen, jedoch wäre eine Klärung des Status von PKS-Crypt hilfreich, da damit eine amtliche Bestätigung für viele der in [RegTP02a] formulierten Anforderungen gegeben wird und in der Bestätigung die genauen Einsatzbedingungen formuliert werden.

- Wartungsarbeiten und Reparaturen am Archivserver sind durch das technische Personal nur nach Absprache mit einem für den Archivserver berechtigten Mitarbeiter durchzuführen.

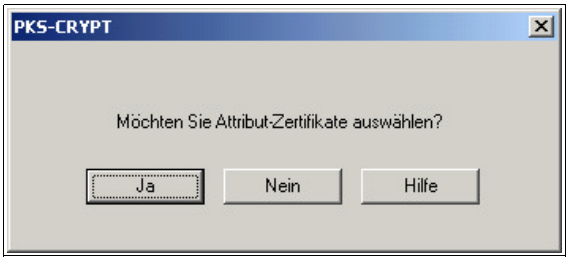
Die Konfiguration des Archivservers ist wie beschrieben zu dokumentieren.

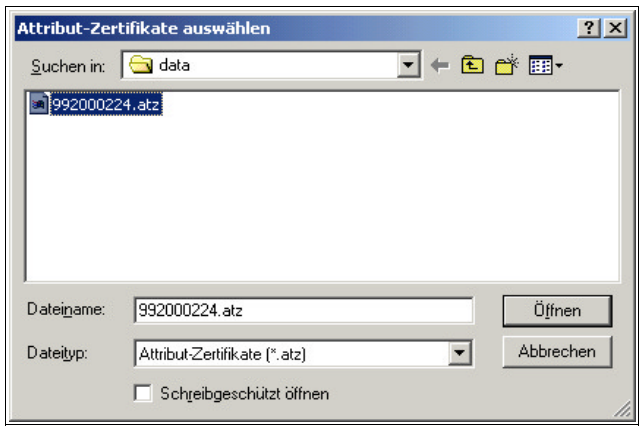
4.3.9 Erstellung der Signaturen und Zeitstempel

Nach der Generierung der Archiv-Sicherungsdateien werden diese signiert. Über der Signatur wird ein Zeitstempel angebracht, um den Signaturzeitpunkt authentisch festzuhalten. Der folgende Abschnitt beschreibt die Nutzung von PKS-Crypt in der Version 1.3 zur Erstellung der Signaturen und Zeitstempel.

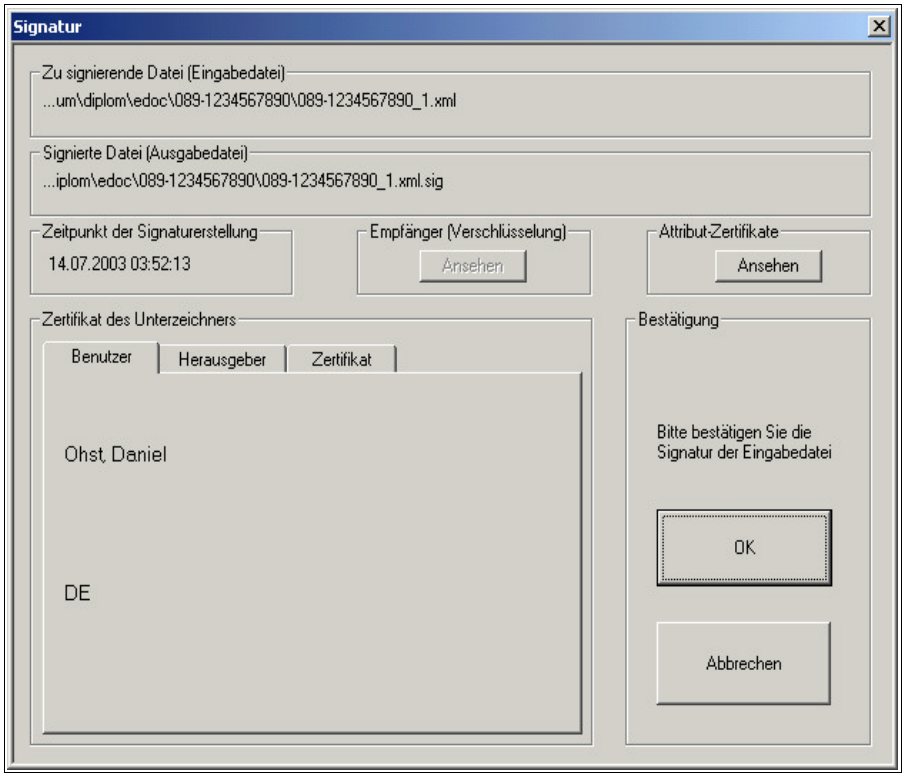
Vor dem Beginn des Vorgangs ist die Internetverbindung zu aktivieren, um den Zeitstempeldienst kontaktieren zu können. Dabei ist auf korrektes Funktionieren der bereits erwähnten Firewall-Funktionen zu achten.

Da die Anwendung sich in den Windows-Explorer integriert, kann auf dem Archivserver direkt in das Verzeichnis mit der ASD gewechselt werden. Mit der rechten Maustaste wird zunächst die Funktion „Signatur erstellen“ aufgerufen, da eine Kombination Signatur/Zeitstempel derzeit nicht unterstützt wird. Nach Eingabe der PIN zur Freischaltung der Chipkarte wird zunächst das Attributzertifikat für die Selbstbeschränkung ausgewählt.





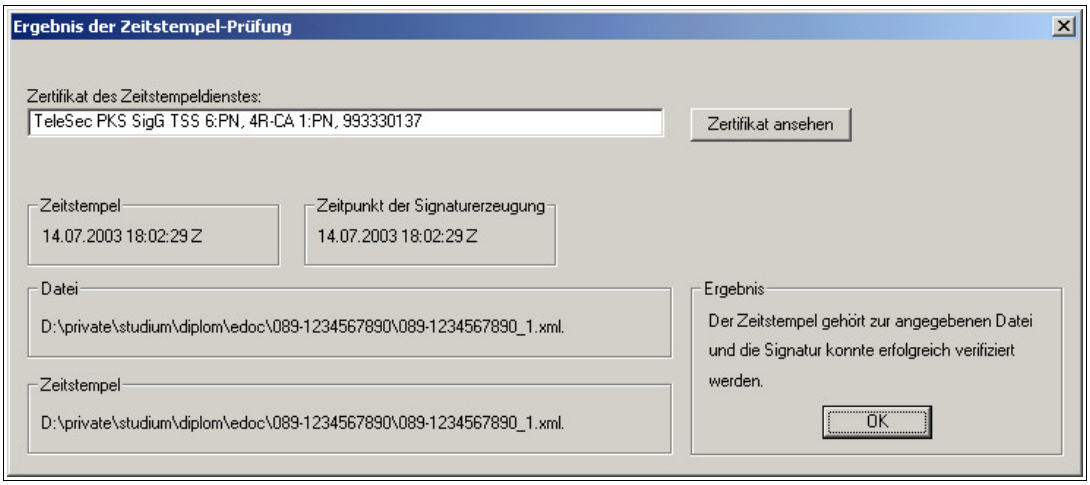
Das Attributzertifikat wird unterhalb des Programmverzeichnisses von PKS-Crypt im Verzeichnis cert_server/data gespeichert. Anschließend erscheint das Fenster mit Informationen zur zu erstellenden Signatur:



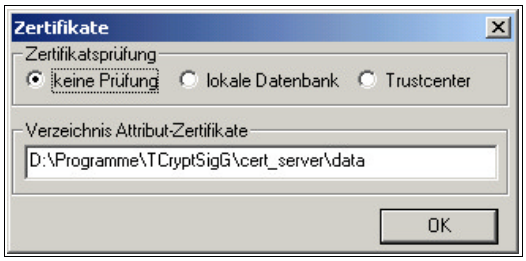
Im Ergebnis entsteht eine Datei mit dem gleichen Dateinamen wie die Originaldatei ergänzt um die Endung .sig. Diese wird jetzt mit dem Zeitstempel versehen. Dazu wird die Funktion „Zeitstempel erzeugen“ im Kontextmenü der gerade erstellten Signaturdatei aufgerufen. Es erscheint insgesamt dreimal das folgende Bestätigungsfenster:

Damit wird das Absenden der Zeitstempel-Anfrage an den Server sowie der Erhalt des Zeitstempels bestätigt. Es wird geprüft, ob der Nutzer berechtigt ist, den Zeitstempeldienst in Anspruch zu nehmen. Es erfolgt keine weitere Meldung, sondern es wird eine Datei mit der Endung .tsm abgelegt, die den Zeitstempel enthält.

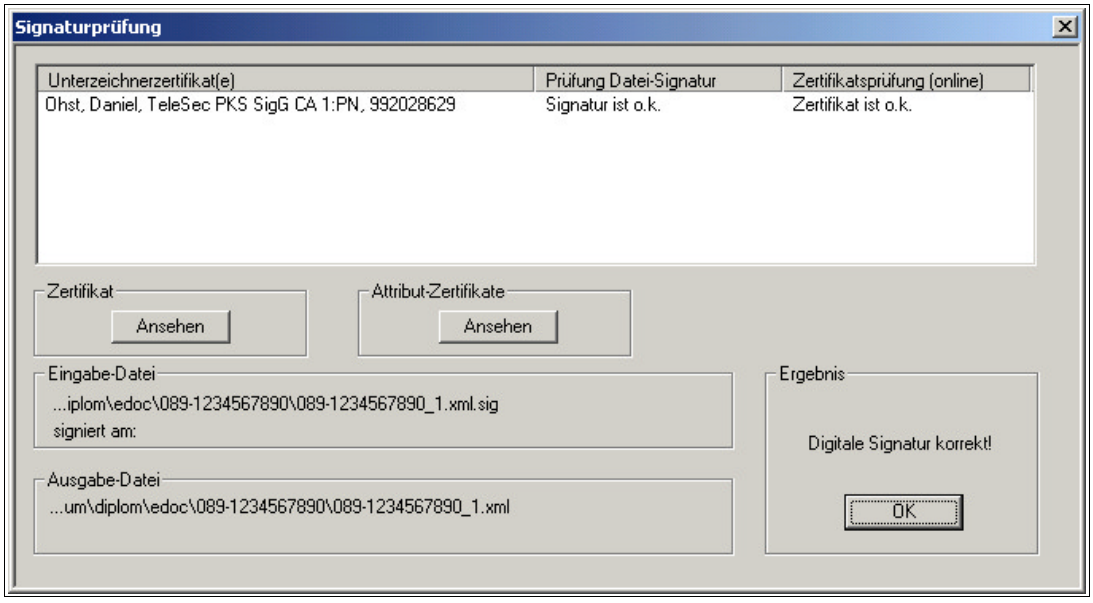
Die Prüfung erfolgt analog mit dem Aufruf der Funktion „Zeitstempel prüfen“ im Kontextmenü der tsm-Datei. Anschließend ist als Ursprungsdatei die Signaturdatei auszuwählen. Bei erfolgreicher Prüfung erscheint das folgende Fenster, das bestätigt, dass der Zeitstempel zu der angegebenen Datei erzeugt wurde und die Signatur des Zeitstempeldienstes korrekt ist.



Die Prüfung der Signaturdatei erfolgt durch Aufruf der Funktion „Signatur prüfen“ im Kontextmenü. Es erscheint ein Auswahlfenster mit mehreren Optionen zur Prüfung des Signaturzertifikats.



Grundsätzlich sollte immer online im Trustcenter geprüft werden, da nur so sichergestellt ist, dass Sperrlisteneinträge korrekt berücksichtigt werden. Es müssen zwei Signatur-Bestätigungen an das Trustcenter gesendet werden. Da die Signaturdatei in der derzeitigen Version von PKS-Crypt auch die Originaldatei enthält, wird diese standardmäßig im aktuellen Verzeichnis abgelegt. Falls sie dort schon vorhanden sein sollte, erscheint eine Sicherheitsabfrage. Schließlich erscheint das Fenster mit der Signaturprüfung und der Anzeige, ob die Signatur selbst und die zugrunde liegende Zertifikatskette gültig sind.



4.3.10 Geschäftsvorfälle

Im Rahmen der Publikation von Dissertationen und anderen Arbeiten wurde bereits ein komplexer Geschäftsgang von der Abgabe der Arbeit durch den Autor über die Konvertierung in verschiedene Zielformate bis zur Veröffentlichung auf dem Dokumentenserver der HU definiert. Im Folgenden werden Geschäftsvorfälle aufgeführt, die im Zusammenhang mit der Authentizitäts- und Integritätssicherung der Dokumente stehen. Es werden die durchzuführenden Schritte und die Einordnung in den übergeordneten Geschäftsgang betrachtet.

Die Geschäftsvorfälle, die im Rahmen der Langzeitarchivierung relevant sind – der Verlust der Sicherheitseignung der eingesetzten Signatur- bzw. Hash-Algorithmen – werden hier nicht detailliert betrachtet. Die derzeitig eingesetzten Signatur- und Hash-Algorithmen sind nach Einschätzung der RegTP auch noch Ende 2008 gültig [Regtp01]. Es ist also sehr unwahrscheinlich, dass in den nächsten Jahren eine Neusignatur von in diesem Projekt erzeugten Dateien notwendig sein wird. Es werden sich zukünftig Standards und Produkte für die Verarbeitung von elektronischen Signaturen entwickeln, die auch die Problematik der Langzeitarchivierung abdecken. Diese Entwicklungen sind zu verfolgen und das Konzept ggf. anzupassen. Es sei jedoch angemerkt, dass mit dem hier vorgestellten Konzept einer Archiv-Sicherungsdatei schon gute Voraussetzungen für eine notwendige Erneuerung von Signaturen geschaffen worden sind. So muss im Falle des Unsicherwerdens des Signaturalgorithmus, nur die ASD unter Einschluss alter Signaturen signiert werden. Ein Zugriff auf die archivierten Dateien ist nicht erforderlich, so dass diese Neusignatur auch einen externen Diensleister ausgelagert werden könnte. Bei Unsicherwerden des Hash-Algorithmus müssen die Dateien mit dem neuen Algorithmus gehasht und dann neu signiert werden. Da dieses Verfahren relativ aufwendig ist, könnte z.B. jede Datei mit einem zweiten Hash-Algorithmus gehasht und dieser Wert zusätzlich in die ASD eingetragen werden. Dadurch wäre eine Neuerstellung der ASD nur dann erforderlich, wenn diese zwei Algorithmen gleichzeitig unsicher werden, was sehr unwahrscheinlich sein dürfte.

4.3.10.1 Erstellung von Signaturen

Die Erstellung von Signaturen und Zeitstempeln erfolgt immer im Zusammenhang mit der Erstellung einer Archiv-Sicherungsdatei. Die erstmalige Erstellung sollte unmittelbar nach Abgabe der Originaldateien des Autors durchgeführt werden, um einen Nach-

weis für die elektronische Abgabe zu besitzen. Weitere ASD werden nach durchgeführten Konvertierungen in die Zielformate, bei Verfügbarkeit und Änderung von Metadaten sowie im Rahmen der Langzeitarchivierung bei Konvertierungen in neue verfügbare Formate erstellt.

Zunächst sind die zu archivierenden Dateien auf das Transferlaufwerk zu kopieren, damit vom Archivserver darauf zugegriffen werden kann. Der Archivserver wird dann gestartet. Es ist auf eine korrekte Funktion der Sicherungsmaßnahmen, insbesondere der installierten Firewall-Software zu achten. Die Dateien werden vom Transferlaufwerk in die Archivierungsstruktur übertragen. Falls noch keine vorhanden ist, kann diese z.B. aus einem Template erzeugt werden, das nur die oben beschriebenen Ordner enthält. Dazu ist natürlich die vorherige Vergabe eines URN für das Dokument notwendig. Alle zu archivierenden Dateien sind gemäß Verfahrensanweisung mit dem dokumentierten Viewer zu betrachten, falls dies nicht in geeigneter Weise schon auf dem Mitarbeiter-PC durchgeführt wurde.

Anschließend ist die Archiv-Sicherungsdatei zu erzeugen. Diese Aufgabe ist gut automatisierbar und kann über ein Skript erfolgen, das die Dateien einsammelt, einen MIME-Type vorschlägt, den Hash-Wert berechnet und die festen Bestandteile der ASD einfügt. Die variablen Angaben zu Autor, Titel, Grund der Erstellung usw. können leicht über ein Formular abgefragt werden.

Die automatisch generierte ASD sollte noch einmal manuell auf Richtigkeit geprüft werden. Dann wird das Programm PKS-Crypt gestartet und die Signatur für die ASD erstellt. Dabei ist auf die Einbeziehung des Attributzertifikats zu achten. Danach kann der Zeitstempel für die Signaturdatei beim ZDA angefordert werden.

Somit ist der Archivierungsvorgang für dieses Dokument abgeschlossen und es können bei Bedarf weitere bearbeitet werden. Bevor der Archivserver dann wieder abgeschaltet werden kann, muss eine Sicherung der Daten auf das zentrale Backup-System initiiert werden.

4.3.10.2 Prüfung von Archiv-Sicherungsdateien

Zur kompletten Prüfung einer ASD ist der Zugriff auf die Signaturen und Zeitstempel, die ASD selbst sowie die referenzierten Archiv-Dateien notwendig. Diese sind bei Bedarf aus dem zentralen Backup-System zu beziehen.

Die Prüfung erfolgt in drei Stufen:

1. Prüfung der Gültigkeit des Zeitstempels

   Diese erfolgt mit PKS-Crypt. Damit kann bei Erfolg nachgewiesen werden, dass die Signatur über der ASD spätestens zum angegebenen Zeitpunkt erzeugt worden ist.

2. Prüfung der Gültigkeit der Signatur
   Hier kommt ebenfalls PKS-Crypt zum Einsatz. Da die Anwendung derzeit nicht in der Lage ist, auf den Signaturzeitpunkt zu prüfen, ist bei abgelaufener Gültigkeitsdauer des zugrunde liegenden Zertifikats kein positives Ergebnis zu erwarten. Alternativ kann die mathematische Prüfung der Signatur durchgeführt und zur Zertifikatsprüfung eine zeitgestempelte OCSP-Antwort herangezogen werden.

3. Prüfung der Hash-Werte der in der ASD referenzierten Dateien
   Es werden die Hash-Werte über die Archiv-Dateien gebildet und mit den Werten in der ASD verglichen. Wenn jeder Wert übereinstimmt und alle Dateien vorhanden sind, ist die Prüfung erfolgreich.

4.3.10.3 Zeitlicher Ablauf eines Zertifikats

Die Gültigkeit von Zertifikaten ist nach den Vorgaben der Signaturverordnung auf maximal 5 Jahre beschränkt und muss innerhalb des Gültigkeitszeitraums der zugrunde liegenden kryptografischen Algorithmen liegen. Beim Anbieter Telesec ist die Gültigkeit derzeit auf 3 Jahre begrenzt. Vor dem regulären Ablauf wird die neue Karte durch den Anbieter automatisch neu verschickt. Nach der Freischaltung ist auf einem Formular der Erhalt schriftlich gegenüber Telesec zu bestätigen. Erst danach wird das Zertifikat in das Verzeichnis aufgenommen und darf genutzt werden.

Die Ausgabe der neuen Chipkarte ist wie unter dem Punkt Dokumentation beschrieben festzuhalten. Die alte Karte wird zurückgegeben und unbrauchbar gemacht. Die Gültigkeit der mit dem alten Signaturschlüssels erzeugten Signaturen bleibt hiervon unberührt.

4.3.10.4 Kompromittierung des Signaturschlüssels

Durch die Speicherung des Signaturschlüssels in der Hardware der Chipkarte wird ein Auslesen des Schlüssels wirksam verhindert. Signaturoperationen können nur nach Eingabe der PIN auf der Karte selbst durchgeführt werden. Eine Kompromittierung durch

direkten Zugriff auf den Schlüssel ist also sehr unwahrscheinlich. Eine Kompromittierung tritt jedoch auch dann ein, wenn die PIN Unbefugten bekannt geworden ist und nicht ausgeschlossen werden kann, dass diese auch Zugriff auf die Chipkarte erlangt haben. In diesen Fällen ist eine Sperrung des Zertifikats vorzunehmen. Die Sperrung kann durch den Mitarbeiter selbst oder auch die Organisation selbst erfolgen. Sie kann durch eine signierte Sperranforderung an den ZDA, telefonisch unter Angabe des Telepassworts oder auch schriftlich erfolgen. Das Zertifikat wird auf die Sperrliste des Anbieters gesetzt. Nachträglich erstellte Signaturen sind nicht mehr gültig, zuvor erstellte Signaturen bleiben weiterhin gültig. Die Chipkarte ist unbrauchbar zu machen (z.B. durch Shreddern oder Ausstanzen des Chips), um zu verhindern, dass weiterhin mit ihr signiert wird. Die Sperrung und der Grund sind zu dokumentieren. Falls der betroffene Mitarbeiter weiterhin berechtigt ist, Signaturen zu erzeugen, ist eine neue Karte beim ZDA zu beantragen.

Eine Sperrung des Zertifikats durch die Organisation ist auch dann vorzunehmen, wenn der Verdacht besteht, dass der Mitarbeiter die Chipkarte missbräuchlich verwendet hat.

4.3.10.5 Vergessene PIN

Entsprechend der Verfahrensregelung sind die von den Mitarbeitern gewählten PINs sicher bei der Verwaltungsleitung zu hinterlegen, um nicht jedesmal neue Karten ausstellen zu müssen, nur wenn eine PIN vergessen wurde. Insofern wird diesem Fall wirksam vorgebeugt. Falls aus irgendwelchen Gründen die PIN nicht korrekt hinterlegt wurde, ist die Chipkarte entsprechend unbrauchbar zu machen. Eine Sperrung des Zertifikats ist nicht notwendig, da keine Kompromittierung vorliegt.

4.3.10.6 Ausscheiden eines Mitarbeiters aus der Organisation

Falls ein Mitarbeiter die Organisation verlässt, ist die Chipkarte durch ihn an die Verwaltungsleitung zurückzugeben, die sie unbrauchbar macht. Der PIN-Brief ist ebenfalls zu vernichten. Eine Sperrung des Zertifikats ist nicht notwendig, da keine Kompromittierung vorliegt.

4.3.10.7 Beendigung der Tätigkeit des Zertifizierungsdiensteanbieters

Das Signaturgesetz regelt im §13 das Verfahren bei Einstellung der Tätigkeit eines Zertifizierungsdiensteanbieters. Im Falle eines akkreditierten Anbieters gilt zusätzlich §15

(6). Danach ist die Einstellung der Tätigkeit der zuständigen Behörde anzuzeigen; die Signaturschlüsselinhaber sind zu informieren. Falls kein anderer akkreditierter Anbieter der Übernahme der Verträge zustimmt, ist dafür die zuständige Behörde verantwortlich, ebenso wie für die Übernahme der Dokumentation gemäß §10 (1).

Rein rechtlich ist also die korrekte Abwicklung der Verträge und damit die korrekte Signaturerstellung weiterhin gewährleistet. Der konkrete Fall ist jedoch erst einmal eingetreten, und zwar als die Deutsche Post im Jahre 2002 die Einstellung ihres Dienstes Signtrust bei der RegTP bekannt gab, ohne jedoch einen genauen Termin zu nennen. Die Anzeige wurde wenig später wieder zurückgezogen, wahrscheinlich aufgrund von möglichen Schadenersatzklagen bereits existierender Kunden, wie z.B. der Medizon AG und von Bundesnotarkammern. Die Rücknahme der Einstellungsanzeige erfolgte auch vor der Übernahme der Zertifikate und der Dokumentation durch einen anderen Dienstleister, so dass bisher keine praktischen Erfahrungen vorliegen. Falls ein ZDA seinen Betrieb einstellt, können die bisherigen Chipkarten weiter genutzt werden. Der neue Zertifizierungsdiensteanbieter bzw. die RegTP hat die Kunden über Änderungen, wie z.B. die Ausgabe neuer Chipkarten, die Verfügbarkeit neuer Signaturanwendungskomponenten, die Änderung von Serveradressen usw., zu informieren. Es kann also nur empfohlen werden, aufmerksam die Veröffentlichungen in Bezug auf die Tätigkeitseinstellung zu verfolgen und in Abhängigkeit davon, die Entscheidung für einen Wechsel zu einem anderen Anbieter oder den Verbleib unter den geänderten Rahmenbedingungen zu treffen.

Wichtig ist, in jedem Falle die langfristige Prüfbarkeit der ausgestellten Signaturen sicherzustellen. Dazu ist ggf. auch die genutzte Software weiterhin vorzuhalten. Im Zuge der Standardisierung der Dienste und Formate mit ISIS-MTT sollte jedoch auch die Prüfung mit anderen Produkten möglich sein. Auch wenn das Zertifikatsverzeichnis von einem neuen Anbieter übernommen werden muss, sollte rechtzeitig für alle existierenden Zertifikate eine zeitgestempelte OCSP-Anfrage eingeholt und archiviert werden.

4.3.11 Migration existierender Signaturen

Der bisherige Einsatz von elektronischen Signaturen und Zeitstempeln für die Dokumentensicherung unterscheidet sich von dem hier vorgeschlagenen Verfahren. Dennoch ist es wichtig, die bereits erstellten Signaturen auch weiterhin verfügbar zu halten und zu archivieren.

Auf dem derzeitigen Archivserver werden die Original-Dateien sowie die konvertierten Versionen aufbewahrt. Alle Originaldateien befinden sich in einem Ordner, der nach folgender Konvention bezeichnet ist: Nachname-Vorname-Original. Die PDF-, SGML- und HTML-Version befindet sich in einem Ordner mit der Bezeichnung „Nachname-Vorname-Archiv." Wenn die Konvertierungen vorliegen und alle Signaturen und Zeitstempel erzeugt wurden, befinden sich dort jeweils ein ZIP-Archiv mit allen Dateien der jeweiligen Version, eine .sig-Datei mit der elektronischen Signatur des ZIP-Archivs sowie eine .tsm-Datei mit dem Zeitstempel über der Signaturdatei. Für einige Dokumente wurden keine Signaturen erzeugt. Diese könnten im Rahmen dieser Migrationsstrategie nachträglich erzeugt werden.

Abbildung 4.7 Alte Archivstruktur

Da die durch PKS-Crypt erzeugten Signaturdateien auch die Originaldatei selbst enthalten, wurde teilweise aus Gründen der Platzersparnis die Originaldatei von den Signaturdateien getrennt. Dabei entstanden drei Dateien: ein Signatur-Header, die Originaldatei sowie ein Signatur-Footer. Es wurden dann nur die vergleichsweise kleinen Signaturteile archiviert. Vor einer Prüfung der Signatur werden die drei Dateien einfach wieder zusammengesetzt. Es muss getestet werden, ob eine neue Version von PKS-Crypt in der Lage ist, sofort getrennte Signaturdateien zu erzeugen.

Eine Variante für die Übernahme der alten Signaturen besteht darin, alle Dateien in die neue Ordnerstruktur zu überführen, anschließend die XML-Struktur zu erweitern, um auch Dateien vom Typ Signatur und ZIP-Archiv aufnehmen zu können, und danach neue Archiv-Sicherungsdateien zu generieren, für die neue Signaturen und Zeitstempel erzeugt werden. Diese Lösung ist sehr aufwändig, da die Überführung in die neue Struktur nur teilweise automatisch vorgenommen werden kann.

Eine effizientere Möglichkeit ist die Nutzung des Konstrukts Archiv-Sicherungsdatei unter Beibehaltung der alten Ordnerstrukturen. Dabei wird ein reduziertes XML-Schema genutzt, das keinen Header mit Informationen zum Dokument und keine MIME-Types enthält. Alle Dateien, die sich in den entsprechenden Ordnern befinden, werden automatisch in der ASD erfasst und mit einem Hash-Wert versehen. Im Anhang C befindet sich das zugehörige XML-Schema. Für den oben abgebildeten Ausschnitt aus der Ordnerstruktur eines Dokuments würde sich folgendes XML-Dokument ergeben:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!-- edited with XMLSPY v5 rel. 2 U (http://www.xmlspy.com) by Daniel Ohst-->
<archive>
    <creation_date>22.09.2003</creation_date>
    <contact>
    Arbeitsgruppe Elektronisches Publizieren
    Humboldt-Universität zu Berlin
    Erwin Schrödinger-Zentrum
    Rudower Chaussee 26
    12489 Berlin
    edoc@cms.hu-berlin.de
    </contact>
    <archivename>mertens-frank</archivename>
    <file>
        <uri>mertens.pdf.sig</uri>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>XUGkuN9XUJ/4kn4bQDUKZuBNQPM=</DigestValue>
    </file>
    <file>
        <uri>mertens.pdf.sig.tsm</uri>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>Yp3NsaxU9ar2nPrDCSpHtagOKCQ=</DigestValue>
    </file>
    <file>
        <uri>original.zip.sig</uri>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>0noTjO7UthEkHEaVWWe049aVwl0=</DigestValue>
    </file>
    <file>
        <uri>original.zip.sig.tsm</uri>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>E67nZwp8u9GMq06xHp2q6mAtsKI=</DigestValue>
    </file>
    <file>
        <uri>sgml.zip.sig</uri>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>10IL3uNr7XjfvFrkturndNmZtC8=</DigestValue>
    </file>
    <file>
        <uri>sgml.zip.sig.tsm</uri>
```

```
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>XuF4zx4+EMPrhXv+LTINcpfiL68=</DigestValue>
    </file>
    <Comment>Migration eines Dokuments.</Comment>
    <Disclaimer>Dieses Dokument ist eine eingeschränkte Archiv-Sicherungsdatei für Dokumente zu Migrationszwecken.
     Fragen zum Inhalt dieses Dokuments werden unter der angegebenen Kontaktadresse beantwortet.</Disclaimer>
</archive>
```

Die Integration von weiteren zu archivierenden Dateien auch in Ordnerstrukturen ist mit diesem Schema problemlos möglich. Die Erstellung kann automatisch erfolgen. Anschließend wird auch nicht jede erzeugte XML-Datei separat signiert und zeitgestempelt, sondern eine Metadatei mit Referenzen auf alle XML-Dateien und ihren jeweiligen Hash-Werten:

```
<metaarchive>

<comment>
Diese Metadatei enthält Referenzen und Hash-Werte der Archiv-Sicherungsdateien, die für die Migration der Signaturen
erstellt wurden.
</comment>

<file>
<uri>mertens-frank.xml</urn>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>3oXexu4pYadHxKdxVaElfmTnmIQ=</DigestValue>
</file>

</metaarchive>
```

Mit dem vorgeschlagenen Migrationskonzept können die bereits vorhandenen Dokumente und die bereits erstellten Signaturen sowie Zeitstempel auf einheitliche Weise übernommen und noch nicht signierte Dokumente nachgetragen werden.

Vorhandene Zertifikate auf den alten Chipkarten sollten baldmöglichst erneuert und damit an die neuen Anforderungen angepasst werden. Chipkarten, die durch vergessene PINs nicht mehr benutzt werden können, sind an die Verwaltungsleitung zurückzugeben und unbrauchbar zu machen. Zertifikate zu Signaturschlüsseln, die eventuell kompromittiert wurden, sind zuvor beim ZDA zu sperren. Die Gültigkeit der bereits erstellten Signaturen bleibt davon unberührt, sofern durch einen Zeitstempel der Zeitpunkt der Erstellung nachweisbar ist.

4.3.12 Verfahrensregelungen und Policy des Dokumentenservers

4.3.12.1 Verfahrensregelungen

Für die Umsetzung des Konzepts ist es erforderlich, dass auch eine Reihe von organisatorischen Regelungen getroffen und dokumentiert wird. Nur so lässt sich eine reibungslose Integration in den Geschäftsablauf unter gleichzeitiger Wahrung eines hohen Sicherheitsstandards erreichen.

Im Folgenden werden Formulierungsvorschläge unterbreitet, die in entsprechende Dokumente eingearbeitet werden können.

1. Verfahrensregelung zum Umgang mit Zertifikaten

Für die Sicherung von Authentizität und Integrität der elektronischen Publikationen, die auf dem Dokumentenserver der Humboldt-Universität zu Berlin veröffentlicht sind, werden qualifizierte Signaturen und Zeitstempel mit Anbieterakkreditierung gemäß dem deutschen Signaturgesetz [SigG01] eingesetzt. Dazu werden Zertifikate für die mit diesen Aufgaben betrauten Mitarbeiter beantragt. Die Zertifikate werden unter dem Namen des jeweiligen Mitarbeiters ausgestellt, wobei der angezeigte Name ein Pseudonym ist, das auch die Referenz auf die Humboldt-Universität enthält. Des weiteren ist eine Selbstbeschränkung einzutragen. Die Beantragung des Zertifikats erfolgt durch die Verwaltungsleitung des CMS und Abstimmung mit der Leitung der „Arbeitsgruppe Elektronisches Publizieren“. Die Ausgabe und Zurücknahme der Chipkarte ist jeweils durch die Verwaltungsleitung zu dokumentieren.

Die Nutzung der Zertifikate ist nur für dienstliche Aufgaben im Rahmen des in der Selbstbeschränkung definierten Spektrums zulässig. Eine private Nutzung ist strikt untersagt. Eine Sperrung des Zertifikats kann jederzeit durch die Verwaltungsleitung auch ohne Mitwirkung des Zertifikatsinhabers erfolgen. Der jeweilige Mitarbeiter ist für die Rechtsfolgen, die aus einer unberechtigten Nutzung des Zertifikats entstehen, in vollem Umfang selbst verantwortlich.

Die Karte ist sorgfältig aufzubewahren. Die nach Freischaltung der Karte gewählte PIN ist vertraulich zu behandeln und insbesondere keiner anderen Person mitzuteilen. Es erfolgt eine Hinterlegung in einem verschlossenen Umschlag bei der Verwaltungsleitung. Jeglicher Hinweis auf einen möglichen Missbrauch ist sofort der Leitung der „Ar-

beitsgruppe Elektronisches Publizieren“ zu melden, die ggf. eine Sperrung des Zertifikats veranlasst. Mit dem Ende der Gültigkeit des Zertifikats oder nach dessen Sperrung ist die Chipkarte der Verwaltungsleitung zu übergeben und unbrauchbar zu machen.

2. Verfahrensregelung zur Archivierung von elektronischen Publikationen

Die Nutzung der ausgestellten Zertifikate ist nur im Rahmen der Archivierung elektronischer Dokumente gemäß dem definierten Geschäftsgang zulässig. Die Erstellung von Signaturen und Zeitstempeln darf nur in der vorgeschriebenen technischen Umgebung und mit den zugelassenen Komponenten des Archivservers erfolgen. Der Einsatz der Chipkarte bzw. des Signaturschlüssels ist zu dokumentieren, z.B. in einem Logfile.

Es ist sicherzustellen, dass alle zu archivierenden Dateien mit einem zum MIME-Type passenden Viewer gemäß aktuell gültiger Liste geprüft wurden. Bei der Neuerstellung von Archiv-Sicherungsdateien sind nur die jeweils geänderten oder neu hinzugekommenen Dateien zu betrachten.

4.3.12.2 Policy

Für den Betrieb des Dokumenten- und Publikationsservers der Humboldt-Universität wurde eine Policy veröffentlicht [EDOC01a], die die Ziele und Arbeitsweise des Systems darstellt sowie technische und organisatorische Rahmenbedingungen vorgibt. Solch eine Policy ist keineswegs Standard, betrachtet man die Angebote digitaler Dokumente deutscher Hochschulen. Sie demonstriert den offiziellen Charakter des Angebots und gewährleistet gegenüber Autoren und Nutzern, dass die Publikationen gemäß definierter und kontrollierter Bedingungen veröffentlicht werden. So wurde die Policy der HU auch von der Medienkommission des Akademischen Senats bestätigt.

In Bezug auf die Langzeitsicherung von Dokumenten werden in der Policy folgende Aussagen getroffen:

1. „Der Dokumenten- und Publikationsserver bietet durch besondere Maßnahmen wie digitale Signaturen und Zeitstempel einen Schutz gegen Verfälschungen. Darüber hinaus wird eine Langzeitarchivierung der elektronischen Dokumente gewährleistet“

5.1 „Durch die Vergabe und den Nachweis qualifizierter elektronischer Signaturen erhalten die elektronischen Dokumente ein rechtswirksames Echtheitszertifikat. Die Vergabe der qualifizierten elektronischen Signaturen erfolgt entsprechend dem Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG)“

5.2 „Die elektronischen Dokumente werden mit individuellen und dauerhaften Adressen versehen, welche einen unmittelbaren Zugriff auf die Dokumente erlauben“

5.5 „Bei Verwendung des Formates SGML/XML wird eine Archivierungsgarantie von 50 Jahren gegeben. Die Archivierungsdauer anderer Formate hängt von der Verfügbarkeit des Formates, der Betrachtungssoftware sowie den Konvertierungsmöglichkeiten ab.

Abschnitt 1 enthält die grundsätzliche Aussage, dass Vorkehrungen für die Dokumente getroffen werden, um ihre langfristige Verfügbarkeit zu sichern. Dies wird im Abschnitt 5 konkretisiert, in dem die wesentlichen Anforderungen angesprochen werden, nämlich die Lesbarkeit der Dateien durch Orientierung auf ein konvertierbares Dateiformat, der permanente Zugriff durch eine sich nicht ändernde Internet-Adresse sowie die Sicherung der Integrität und Authentizität der veröffentlichten Dokumente durch qualifizierte Signaturen.

Die Aussage des Absatzes 5.1 ist auch unter Berücksichtigung der Ergebnisse dieser Arbeit weiterhin gültig; allerdings könnte eine präzisere Formulierung noch besser die Vorteile des verwendeten Verfahrens demonstrieren. Im Folgenden wird eine Neufassung des Absatzes vorgeschlagen, die bei einer Überarbeitung der Policy berücksichtigt werden könnte:

Zur Sicherung von Authentizität und Integrität der elektronischen Dokumente werden qualifizierte Signaturen und Zeitstempel mit Anbieterakkreditierung gemäß dem deutschen Signaturgesetz eingesetzt. Die langfristige Prüfbarkeit der Signaturen wird gewährleistet. Die aktuell gültigen technischen und organisatorischen Rahmenbedingungen werden auf dem Dokumentenserver veröffentlicht.

4.3.13 Dokumentation

Um jederzeit den Nachweis der korrekten Umsetzung der in diesem Konzept formulierten Anforderungen führen zu können, ist eine Reihe von Dingen zu dokumentieren:

- Die Ausgabe sowie Sperrung oder Rückgabe der Zertifikate für die Mitarbeiter
- Die für die Signaturerstellung genutzte Software sowie die technische Umgebung des Archivservers
- Die für die Betrachtung der Dateien des Archivs gemäß zugeordnetem MIME-Type definierte Viewer-Software

Die Dokumente sind von der Leitung der „Arbeitsgruppe Elektronisches Publizieren“ zu führen und ständig zu aktualisieren. Sie werden gemäß dem Vorschlag für die Policyänderung auf dem Dokumentenserver veröffentlicht.

1. Zertifikatsverzeichnis

Die Ausgabe und Rücknahme der Chipkarten mit den Zertifikaten erfolgt durch die Verwaltungsleitung. Das Verzeichnis enthält Informationen darüber, wann Mitarbeiter eine Chipkarte für das Signieren elektronischer Dokumente erhalten oder diese

zurückgegeben haben. Im Einzelnen sollen folgende Daten erfasst werden:

Eintrag	Beschreibung
Datum	
Seriennummer der Chipkarte	Die 19-stellige Seriennummer bei den aktuellen Karten der Telesec befindet sich unten vorn.
Name des Mitarbeiters	Entspricht dem Namen des Mitarbeiters, auf den das Zertifikat ausgestellt wurde.
Grund des Eintrags	'Ausgabe','Ablauf der Gültigkeit','Verlust der Karte', 'Verlust der PIN','Sonstiger'.
Unterschrift MA	
Unterschrift Verwaltungsleitung	
Bemerkungen	Kommentare zum Vorgang, insbesondere bei Grund des Eintrags 'Sonstiger'.

Bei Ausgabe der Karte bestätigt der Mitarbeiter durch seine Unterschrift die Kenntnisnahme von den Verfahrensregelungen zum Einsatz des Zertifikats.
Wenn der Mitarbeiter eine Karte neu erhalten hat, muss diese entsprechend dem vom Zertifizierungsdiensteanbieter vorgegebenen Verfahren freigeschaltet werden. Hierbei wird von Telesec das Nullpin-Verfahren genutzt. Hierbei wird eine spezielle Freischaltungsfunktion genutzt, die nur einmal aufgerufen werden kann. Wenn sich diese Funktion nicht korrekt durchführen lässt, ist dies ein Indiz für eine mögliche missbräuchliche Verwendung. Wenn der Mitarbeiter die PIN erfolgreich geändert hat, ist diese auf einem Blatt Papier zu notieren und in einem Umschlag zu verschließen, der mit dem Namen des Mitarbeiters versehen wird. Dieser PIN-Brief ist unverzüglich der Verwaltungsleitung zu übergeben, die ihn an einem sicheren Ort (z.B. Safe) verwahrt. Vergessene PINs sind die häufigste Ursache für nicht mehr nutzbare Chipkarten. Mit der zentralen Hinterlegung kann dem vorgebeugt werden. Selbstverständlich ist durch die Verwaltungsleitung sicherzustellen, dass Mitarbeiter nur auf ihre eigenen PIN-Briefe Zugriff erhalten.

2. Signaturerstellungsumgebung

Die technische Erstellungsumgebung für die Signaturen ist zu dokumentieren und bei Änderungen anzupassen. Zu den zu pflegenden Angaben gehören:

Eintrag	Beschreibung
Systemhardware	Hardware-Konfiguration des Archivservers. Hier sind nur die potentiell im Rahmen der Signaturfunktion relevanten Parameter aufzuführen, die Größe des Speichers ist hier z.B. nicht unbedingt aufzuführen: • Rechnerarchitektur (PC, MAC, UNIX-WS) • Prozessor, Schnittstellen, vorhandene Wechseldatenträger • Konnektivität, z.B. LAN, WLAN
Systemsoftware	Eingesetztes Betriebssystem mit Patchlevel
Anwendungssoftware	Zusätzlich installierte Anwendungen, z.B. zur Prüfung der Dateien. Auch hier ist die Version sowie ein Patchlevel anzugeben.
Signaturanwendungskomponente	Hier ist die Hardware und Software aufzuführen, die zur Erstellung der Signaturen genutzt wird, z.B. • KOBIL-Chipkartenleser B1 Professional HW KCT100 über USB • Telesec PKS-Crypt 1.3 für Windows
Schutz des Systems	Es werden alle zusätzlichen für den Schutz des Systems getroffenen Vorkehrungen aufgeführt: • Zutrittsregelung zum Archivserver • Zugangregelung (Accountverwaltung) • Maßnahmen für die Netzsicherheit, wie z.B. physikalische Abtrennung, Einsatz von Firewall-Software inkl. deren Konfiguration

3. Viewer-Software

Die für die Betrachtung der einzelnen Dateien des Dokuments genutzte Software ist für jeden gemäß Definition der Archiv-Sicherungsdatei gültigen MIME-Type anzugeben und natürlich regelmäßig anzupassen. Es ist ein Hinweis zu eventuellen Abweichungen in den Softwareversionen zwischen der Referenz auf dem Archivserver und den Arbeitsplatzrechnern der mit der Bearbeitung betrauten Mitarbeiter aufzuführen. Eine mögliche Softwareliste findet sich in der folgenden Tabelle:

MIME-Type	Verwendete Software
application/java	Internet Explorer 6
application/msword	MS Word 2000
application/octet-stream	
application/pdf	Acrobat Reader 5.05
application/postscript	Acrobat Reader 5.05
application/wordperfect	WordPerfect 2000
application/x-compressed	Winzip 8.0
application/x-latex	
audio/mpeg3	Windows Media Player 8
audio/wav	Windows Media Player 8
image/jpeg	Internet Explorer 6
image/png	Internet Explorer 6
model/vrml	Internet Explorer 6
text/css	Internet Explorer 6
text/html	Internet Explorer 6
text/plain	Internet Explorer
text/richtext	MS Word 2000
text/sgml	
text/xml	
video/avi	Windows Media Player 8
video/mpeg	Windows Media Player 8

4.3.14 Implementationshinweise

Die Erstellung der Ordnerstruktur für die Dokumente sowie der Archiv-Sicherungsdatei lässt sich weitgehend automatisieren. Auch wenn im Rahmen dieses Konzepts keine diesbezügliche Implementation vorgenommen wurde, sollen dennoch einige Hinweise zu einer möglichen Umsetzung in eine entsprechende Software gegeben werden.

- Die Ordnerstruktur für einen Archiveintrag kann als Template hinterlegt werden. Ein Programm könnte dann z.B. nur noch den URN für den neu zu erstellenden Eintrag abfragen, daraufhin den letzten Counter ermitteln und die neue Struktur erzeugen.
- Die Erstellung der Archiv-Sicherungsdatei lässt sich ebenfalls weitgehend automatisieren. Einige Inhalte können selbstständig ermittelt, andere durch einfache Nutzereingabe abgefragt werden. Beim Durchlaufen der Ordnerstruktur werden für jede gefundene Datei die Einträge mit URI, Hash-Wert und dem MIME-Type erzeugt, der aus einer Tabelle mit den dazugehörigen Dateiendungen ermittelt werden kann. Trotzdem ist die Datei natürlich noch einmal manuell zu überprüfen.
- Die Hash-Werterzeugung kann z.B. mit Hilfe von Programmen aus der OpenSSL-Bibliothek vorgenommen werden. OpenSSL ist ein weltweites Projekt, das es sich unter anderem zum Ziel gesetzt hat, eine frei verfügbare Bibliothek von kryptografischen Funktionen auch für kommerzielle Anwendungen bereitzustellen. Die Software liegt derzeit in der Version 0.9.7b vor und ist Teil vieler Produkte und kann für diese Zwecke als Referenz und damit als hinreichend vertrauenswürdig angesehen werden. Für die Hash-Werterzeugung wird das Programm sha1 eingesetzt, das z.B. mit folgendem Aufruf den gewünschten Hash-Wert für eine Datei erzeugt:
  >openssl sha1 -sha1 -binary mertens.pdf | openssl base64
  >SHA1(mertens.pdf)= mTjVYmwfASSSTa8QmdqqLSwiQCE=
  Der ermittelte Wert kann dann direkt in die XML-Datei übernommen werden. Das Programm wird von der Kommandozeile aufgerufen, es kann auch die Funktion der bereits vorkompilierten Library ssleay32.lib genutzt werden. Eine Integration in eigene Anwendungen ist somit problemlos möglich.

4.4 Bewertung und Weiterentwicklung

Die vorgeschlagene Lösung ist in der Lage, die formulierten Anforderungen zu erfüllen. Sie stellt jedoch eine individuelle Entwicklung dar und ist an einer Reihe von Stellen auf die speziellen Anforderungen bei der Verarbeitung digitaler Dokumente im CMS der HU Berlin und auf eine schnelle Umsetzbarkeit im Rahmen des derzeitigen Workflows optimiert. So orientiert sich z.B. die erstellte Archivierungsstruktur an den derzeit verarbeiteten Dateiformaten und der Ablage von Dateien auf dem Dokumenten- bzw. Archivserver. Dennoch lässt sich das Kernstück der Lösung – die Archiv-Sicherungsdatei – durch die einfache Spezifikation als XML-Schema problemlos an neue Anwendungsfälle anpassen. Die ASD besitzt folgende wesentliche Eigenschaften:

- Durch die Integration aller zu einem Dokument gehörenden Dateien wird die entsprechende Zusammengehörigkeit und eine Vollständigkeitsinformation ausgedrückt.
- Die Zusammenfassung der Referenz auf die Dateien und der Hash-Werte erfordert nur die Erzeugung einer Signatur und eines Zeitstempels.
- Es werden weitere Informationen zum Dokument erfasst, wie Metadaten, die Zugehörigkeit von Dateien zu entsprechenden Dokumentversionen und geprüfte Dateitypen.

Das Grundprinzip einer XML-Datei mit Referenzen auf zugrunde liegende Dokumente wird auch im „Metadata Encoding and Transmission Standard“ der Library of Congress verwendet [METS03]. Das Format erlaubt im Wesentlichen die Erstellung einer XML-Datei mit administrativen und beschreibenden Metadaten über ein Dokument, die Auflistung aller zum Dokument gehörenden Einzeldateien mit Ablageort als URN und weiteren Eigenschaften sowie die Abbildung einer Datei-Hierarchie und Verlinkungen zwischen den Dateien. Der Standard kann somit z.B. zur Implementation eines Archival Information Package gemäß OAIS genutzt werden. METS bietet eine höhere Funktionalität als die in dieser Arbeit vorgestellte Archiv-Sicherungsdatei, dies erfordert jedoch auch einen höheren Aufwand bei der Erstellung und verschlechtert die intuitive Erfassung der Inhalte. Des Weiteren ist derzeit keine Möglichkeit vorgesehen, die Integrität der referenzierten Dateien kryptografisch zu sichern, was jedoch über eine Erweiterung des Standards sicherlich möglich wäre.

Im Projekt „Archisig“, das im Kapitel 3 bereits erwähnt wurde und das sich speziell mit dem Aspekt der Langzeitarchivierung von Signaturen auseinander setzt, werden Hash-Trees zur Zusammenfassung von Dateien genutzt. Eine Abbildung von Dokumenthierarchien ist hierdurch jedoch aufgrund fehlender Flexibilität nicht ohne weiteres möglich. In der ASD sind die referenzierten Dateien linear angeordnet, aber einer oder mehrerer Dokumentversionen, wie z.B. PDF oder SGML, zuordenbar. Auch bei „Archisig“ wird nur eine Signatur bzw. ein Zeitstempel benötigt, um die gesamte Dokumentstruktur zu sichern. Sowohl die ASD als auch das Archisig-Konzept lassen die nachträgliche Löschung von Dateien zu, ohne die Prüfbarkeit insgesamt zu gefährden. Durch den Fokus von „Archisig“ auf die Langzeitarchivierung wurden Konstrukte entworfen, um die Erneuerung von Signaturen und Zeitstempeln signaturgesetzkonform abbilden zu können. Dies wird im Wesentlichen durch die Integration alter Zeitstempel in die Baumstruktur und die anschließende Neusignatur erreicht. Dabei wurde der Fall des Unsicherwerdens des Signaturalgorithmus als auch des verwendeten Hash-Algorithmus berücksichtigt. Die Konzepte werden im Projektrahmen prototypisch umgesetzt und sind teilweise als Vorschläge für die Integration in existierende Standards (ISIS-MTT) eingereicht.

Bereits jetzt gibt es interessante Konzepte und erste Implementationen von Archiv-Systemen, die auch den Aspekt der Langzeitarchivierung berücksichtigen, z.B. das Open Archival Information System (OAIS), das eine modulare Struktur unter Berücksichtigung verschiedener Anforderungen und Rollen im Archivierungsprozess beschreibt [OAIS02]. Im Februar wurde ein Internet Draft zur Spezifikation eines „Trusted Archive Protocol“ vorgelegt [IETF03], der die Langzeitarchivierung kryptografischer Informationen in Archiven betrachtet. Die Entwicklung von solchen Standards aber auch der Markt der kommerziellen Anbieter ist weiter zu beobachten und die Lösung kontinuierlich anzupassen und zu optimieren.

Viele Dokumente enthalten eine Reihe von Abbildungen und Grafiken. Diese werden derzeit einzeln als Objekt in der Archiv-Sicherungsdatei abgelegt. Bei einer hohen Anzahl von Elementen kann die ASD schnell sehr unübersichtlich werden. Eine Möglichkeit der Optimierung wäre eine stärkere Gruppierung der verschiedenen Elemente oder auch eine Auslagerung von bestimmten Dateigruppen, um die ASD klein und übersichtlich zu halten.

Die derzeitig verwendete Signaturanwendungskomponente PKS-Crypt ist hinsichtlich ihrer Bedienerfreundlichkeit und der Transparenz des Signiervorgangs noch optimierbar. So könnten z.B. Präsentationskomponenten integriert werden, um die Darstellung dessen, was zu signieren ist, zu verbessern. Auch eine Erweiterung der Funktionalität ist wünschenswert, wie z.B. die korrekte Prüfung auf den Signaturzeitpunkt oder die integrierte Erstellung von Signatur und Zeitstempel. Durch Standards von Signaturanwendungsumgebungen könnte die Vertrauenswürdigkeit der erstellten Signaturen erhöht werden, da nicht jede Maßnahme im Einzelnen nachgewiesen und bewertet werden müsste, die zum Schutz des Archivservers umgesetzt wurde. Weitere Fortschritte sind bei praktischen Verfahren für die Langzeitarchivierung von Signaturen zu erwarten. Durch die Integration von Signaturkomponenten in Archivsysteme oder auch durch Nutzung der Dienstleistungen kommerzieller Archivierungsdienste müssen diese Aufgaben künftig nicht mehr manuell durchgeführt werden. Die Ergebnisse des Projekts „Sichere Signaturerstellungsumgebung“ [TC03], das derzeit von der TC Trustcenter AG im Auftrag des BSI realisiert wird, sind bei der Konfiguration des Archivservers zu berücksichtigen.

Mit der Umsetzung von Standards für Signaturen, wie z.B. ISIS-MTT, werden Applikationen verfügbar sein, die interoperabel zu den Strukturen anderer ZDA arbeiten und deren Nutzung nicht abhängig von einer vertraglichen Bindung zum jeweiligen Anbieter ist. Derzeit lässt sich die Anwendung PKS-Crypt selbst für die Prüfung von Signaturen nur dann nutzen, wenn man eine Chipkarte der Telesec besitzt. Dies ist technisch jedoch nicht erforderlich. Bei Verfügbarkeit von offenen Applikationen könnten die Archiv-Sicherungsdatei sowie die erstellten Signaturen und Zeitstempel veröffentlicht werden, so dass die Nutzer des Dokumentenservers in der Lage sind, Prüfungen auf Authentizität und Integrität der ihnen vorliegenden Dateien selbst durchzuführen. Dies würde die Transparenz der durchgeführten Maßnahmen zur Sicherung der Dokumente wesentlich erhöhen.

Die Nutzung der elektronischen Signaturen könnte zukünftig für eine Reihe weiterer Aufgaben im Rahmen Publikationsprozesses genutzt werden. So könnte z.B. die Abgabebescheinigung für den Autor, die derzeit durch CMS erstellt wird, um die vollständige und korrekte Abgabe der elektronischen Dokumentenversion nachzuweisen, als signierte E-Mail an die Bibliothek verschickt werden. Des Weiteren könnte die Kommunikation zwischen verschiedenen Organisationseinrichtungen der Universität vollständig

auf elektronischem Wege erfolgen, z.B. mit den Prüfungsämtern. Für viele dieser Aufgaben wird es nicht erforderlich sein, qualifizierte Signaturen mit Anbieterakkreditierung zu verwenden. Die Nutzung einfacher oder fortgeschrittener Signaturen einer selbst betriebenen PKI mit einem von allen Beteiligten akzeptierten Sicherheitsniveau ist durchaus möglich. Bei der Erweiterung des Einsatzspektrums ist auch die Verschlüsselung von Daten zu berücksichtigen. Eine elektronische Signatur allein schützt nicht die Vertraulichkeit der übertragenen Daten, wie es z.B. für den Austausch von Gutachten oder Prüfungsunterlagen erforderlich ist.

Mit elektronischen Publikationen ergeben sich völlig neue Darstellungsmöglichkeiten, die durch papiergebundene Dokumente nicht erreicht werden, wie z.B. Videos, Audios oder andere multimediale Elemente. Weiterhin können auch dynamische Dokumente erzeugt werden, deren konkrete Erscheinungsform erst durch den Betrachter und die Auswertung von übergebenen Parametern bestimmt wird. So können z.B. - basierend auf in einer Datenbank gespeicherten Messwerten - statistische Auswertungen erzeugt und als Grafiken dargestellt werden. Für eine Archivierung müssten die Datenbankstruktur und die Inhalte, die Programme zur Erzeugung der Auswertungen und Angaben zur Präsentation gespeichert werden. Um eine langfristige Integritätssicherung auf dieser Ebene erzeugen zu können, sind geeignete Speicherstrukturen zu entwickeln.

5 Zusammenfassung

Elektronische Publikationen haben sich in den letzten Jahren als eigenständige Publikationsform etabliert und sind fester Bestandteil wissenschaftlicher Arbeit in vielen Fachgebieten geworden. Deshalb sind Konzepte und Verfahren zu entwickeln, um sie auch langfristig der Allgemeinheit zur Verfügung zu stellen. Während bei der Archivierung gedruckter Publikationen langjährige praktische Erfahrungen und vor allen Dingen etablierte Vorgehensweisen zu sicheren Aufbewahrung über lange Zeiträume existieren, gibt es für elektronische Dokumente dazu im wesentlichen theoretische Überlegungen und individuelle praktische Erfahrungen über vergleichsweise viel kürzere Zeiträume. Im Rahmen dieser Arbeit wurde ein kleiner Teilaspekt der Gesamtproblematik Langzeitarchivierung betrachtet – die Sicherung von Authentizität und Integrität elektronischer Publikationen.

Durch den Einsatz elektronischer Signaturen und Zeitstempel kann sichergestellt werden, dass Dokumente zu einem bestimmten Zeitpunkt einer Person oder Organisation vorgelegen haben und dass langfristig prüfbar ist, dass die Dokumente danach nicht mehr verändert wurden. Die grundlegenden mathematischen Grundlagen, technischen Konzepte von Signaturen sowie die rechtlichen Rahmenbedingungen ihres Einsatzes wurden dargestellt.

Am Beispiel der auf dem Dokumentenserver der Humboldt-Universität zu Berlin veröffentlichten Hochschulpublikationen, insbesondere Dissertationen, wurde ein Konzept für die Authentizitäts- und Integritätssicherung entwickelt. Kernstück der Lösung ist die Definition einer Archiv-Sicherungsdatei, die alle zu einem Dokument gehörenden Dateien referenziert und deren Integrität mit einer qualifizierten Signatur und einem qualifizierten Zeitstempel gemäß deutschem Signaturgesetz sichert. Dabei können Änderungen an den Dokumenten, wie sie z.B. durch Konvertierungen in andere Dateiformate entstehen, berücksichtigt werden. Es werden die technischen Einsatzbedingungen für die Erstellung der Signaturen sowie organisatorische Voraussetzungen definiert.

Anhang A – Beschluss des Akademischen Senats der HU Berlin zur elektronischen Veröffentlichung von Dissertationen

Der Akademische Senat faßt einstimmig (sonstige MA: einstimmig) mit den vorgeschlagenen Änderungen den Beschluß 16/98:

Der Akademische Senat beschließt folgenden Zusatz zu allen bisher verabschiedeten Promotionsordnungen:

Zusätzlich zu den in den einzelnen Promotionsordnungen genannten Möglichkeiten gilt auch die Ablieferung von vier vollständigen Exemplaren, die auf alterungsbeständigem, holz- und säurefreiem Papier ausgedruckt und dauerhaft haltbar gebunden sind, sowie einer elektronischen Version, deren Dateiformat und Datenträger mit der Universitätsbibliothek abzustimmen sind, als Erfüllung der Pflicht zur Veröffentlichung und Verbreitung der Dissertation.

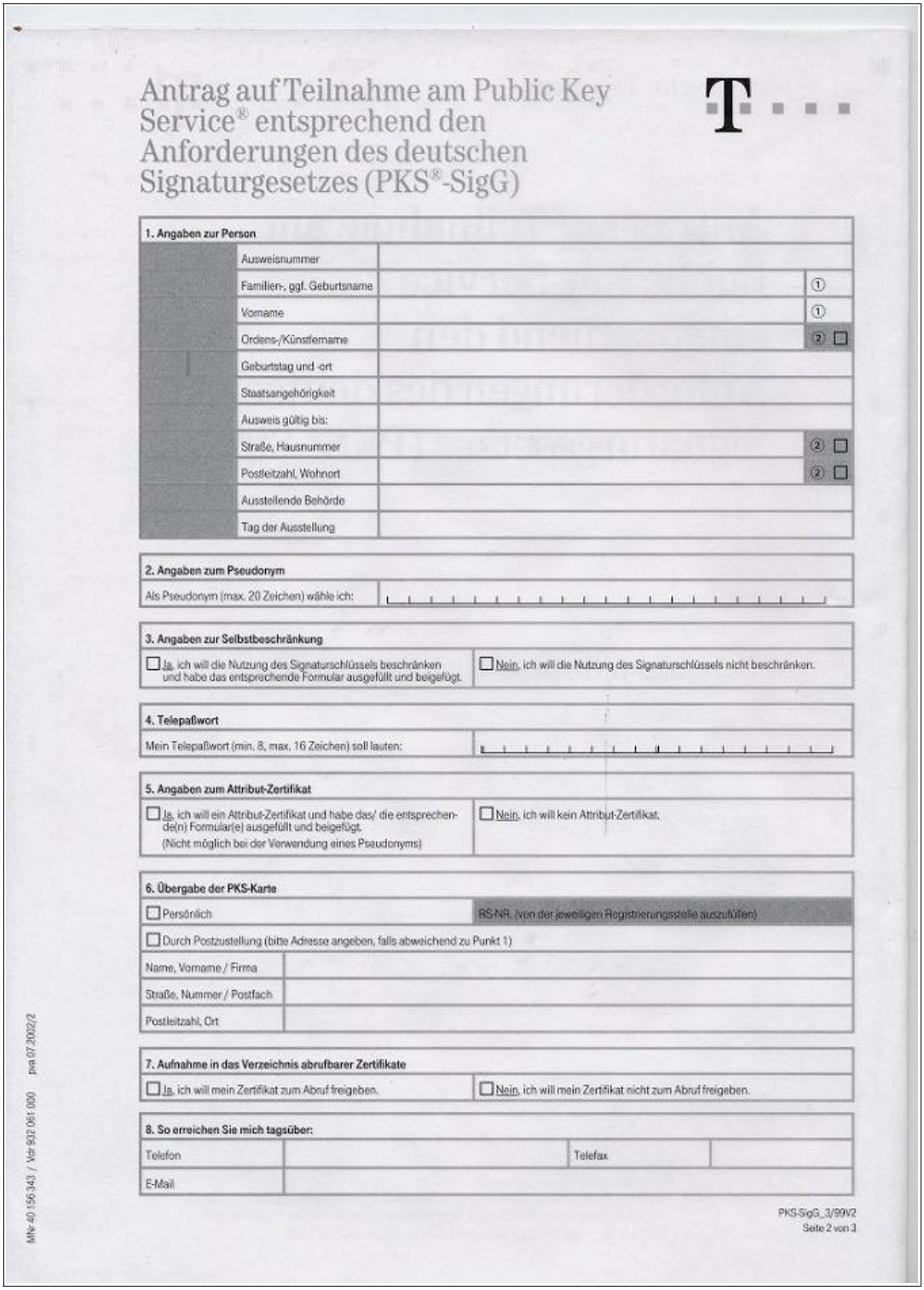
Die Publikation muß ein Abstract in deutscher und englischer Sprache enthalten. Der Doktorand oder die Doktorandin überträgt der Universitätsbibliothek der Humboldt-Universität, der DDB (Die Deutsche Bibliothek) in Frankfurt/Leipzig und ggf. der DFG-Sondersammelgebietsbibliothek das Recht, die elektronische Version in Datennetzen zu veröffentlichen und versichert, daß die elektronische Version der angenommenen Dissertation entspricht. Die Universitätsbibliothek überprüft die abgelieferte Version auf Lesbarkeit und Übereinstimmung mit den geforderten Vorgaben. Die Abgabe von Dateien, die den geforderten Vorgaben hinsichtlich Dateiformat und Datenträger nicht entsprechen, gilt nicht als Veröffentlichung.

Diese Regelung gilt mit ihrem Inkrafttreten zusätzlich zu den in den Promotionsordnungen der Fakultäten getroffenen Festlegungen. Die Fakultäten werden aufgefordert, die Promotionsordnungen entsprechend anzupassen

Den Fakultäten wird empfohlen, auf eine Veröffentlichung von Habilitationsschriften in elektronischer Form hinzuwirken.

Mit der Umsetzung des Beschlusses wird der Präsident beauftragt.

Anhang B - Antragsformulare zur Teilnahme am Telesec Public Key Service



Antrag auf Teilnahme am Public Key Service® entsprechend den Anforderungen des deutschen Signaturgesetzes (PKS®-SigG)

1. Angaben zur Person

Ausweisnummer	
Familien-, ggf. Geburtsname	①
Vorname	①
Ordens-/Künstlername	② ☐
Geburtstag und -ort	
Staatsangehörigkeit	
Ausweis gültig bis:	
Straße, Hausnummer	② ☐
Postleitzahl, Wohnort	② ☐
Ausstellende Behörde	
Tag der Ausstellung	

2. Angaben zum Pseudonym

Als Pseudonym (max. 20 Zeichen) wähle ich:

3. Angaben zur Selbstbeschränkung

☐ Ja, ich will die Nutzung des Signaturschlüssels beschränken und habe das entsprechende Formular ausgefüllt und beigefügt.

☐ Nein, ich will die Nutzung des Signaturschlüssels nicht beschränken.

4. Telepaßwort

Mein Telepaßwort (min. 8, max. 16 Zeichen) soll lauten:

5. Angaben zum Attribut-Zertifikat

☐ Ja, ich will ein Attribut-Zertifikat und habe das/ die entsprechende(n) Formular(e) ausgefüllt und beigefügt.
(Nicht möglich bei der Verwendung eines Pseudonyms)

☐ Nein, ich will kein Attribut-Zertifikat.

6. Übergabe der PKS-Karte

☐ Persönlich — RS-NR. (von der jeweiligen Registrierungsstelle auszufüllen)

☐ Durch Postzustellung (bitte Adresse angeben, falls abweichend zu Punkt 1)

Name, Vorname / Firma	
Straße, Nummer / Postfach	
Postleitzahl, Ort	

7. Aufnahme in das Verzeichnis abrufbarer Zertifikate

☐ Ja, ich will mein Zertifikat zum Abruf freigeben.

☐ Nein, ich will mein Zertifikat nicht zum Abruf freigeben.

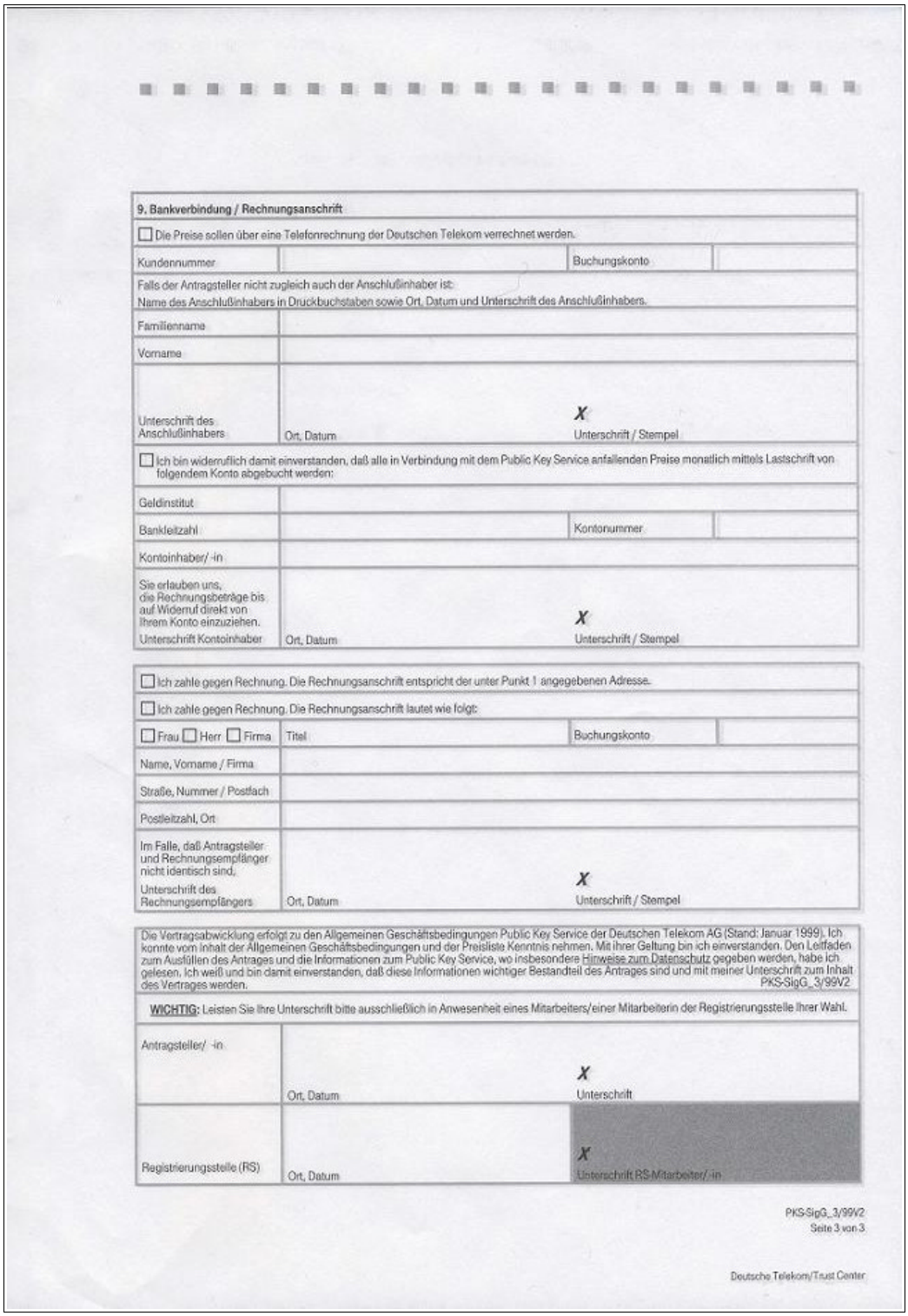
8. So erreichen Sie mich tagsüber:

Telefon		Telefax	
E-Mail			

MNr 40 156 343 / Vdr 932 061 000 pxa 07 2002/2

PKS-SigG_3/99V2
Seite 2 von 3

Abbildung 5.1 Telesec PKS-Antrag Seite 1



9. Bankverbindung / Rechnungsanschrift

☐ Die Preise sollen über eine Telefonrechnung der Deutschen Telekom verrechnet werden.

Kundennummer		Buchungskonto	

Falls der Antragsteller nicht zugleich auch der Anschlußinhaber ist:
Name des Anschlußinhabers in Druckbuchstaben sowie Ort, Datum und Unterschrift des Anschlußinhabers.

Familienname		
Vorname		
Unterschrift des Anschlußinhabers	Ort, Datum	X Unterschrift / Stempel

☐ Ich bin widerruflich damit einverstanden, daß alle in Verbindung mit dem Public Key Service anfallenden Preise monatlich mittels Lastschrift von folgendem Konto abgebucht werden:

Geldinstitut			
Bankleitzahl		Kontonummer	
Kontoinhaber/ -in			
Sie erlauben uns, die Rechnungsbeträge bis auf Widerruf direkt von Ihrem Konto einzuziehen. Unterschrift Kontoinhaber	Ort, Datum	X Unterschrift / Stempel	

☐ Ich zahle gegen Rechnung. Die Rechnungsanschrift entspricht der unter Punkt 1 angegebenen Adresse.

☐ Ich zahle gegen Rechnung. Die Rechnungsanschrift lautet wie folgt:

☐ Frau ☐ Herr ☐ Firma	Titel	Buchungskonto	
Name, Vorname / Firma			
Straße, Nummer / Postfach			
Postleitzahl, Ort			
Im Falle, daß Antragsteller und Rechnungsempfänger nicht identisch sind, Unterschrift des Rechnungsempfängers	Ort, Datum	X Unterschrift / Stempel	

Die Vertragsabwicklung erfolgt zu den Allgemeinen Geschäftsbedingungen Public Key Service der Deutschen Telekom AG (Stand: Januar 1999). Ich konnte vom Inhalt der Allgemeinen Geschäftsbedingungen und der Preisliste Kenntnis nehmen. Mit ihrer Geltung bin ich einverstanden. Den Leitfaden zum Ausfüllen des Antrages und die Informationen zum Public Key Service, wo insbesondere Hinweise zum Datenschutz gegeben werden, habe ich gelesen. Ich weiß und bin damit einverstanden, daß diese Informationen wichtiger Bestandteil des Antrages sind und mit meiner Unterschrift zum Inhalt des Vertrages werden. PKS-SigG_3/99V2

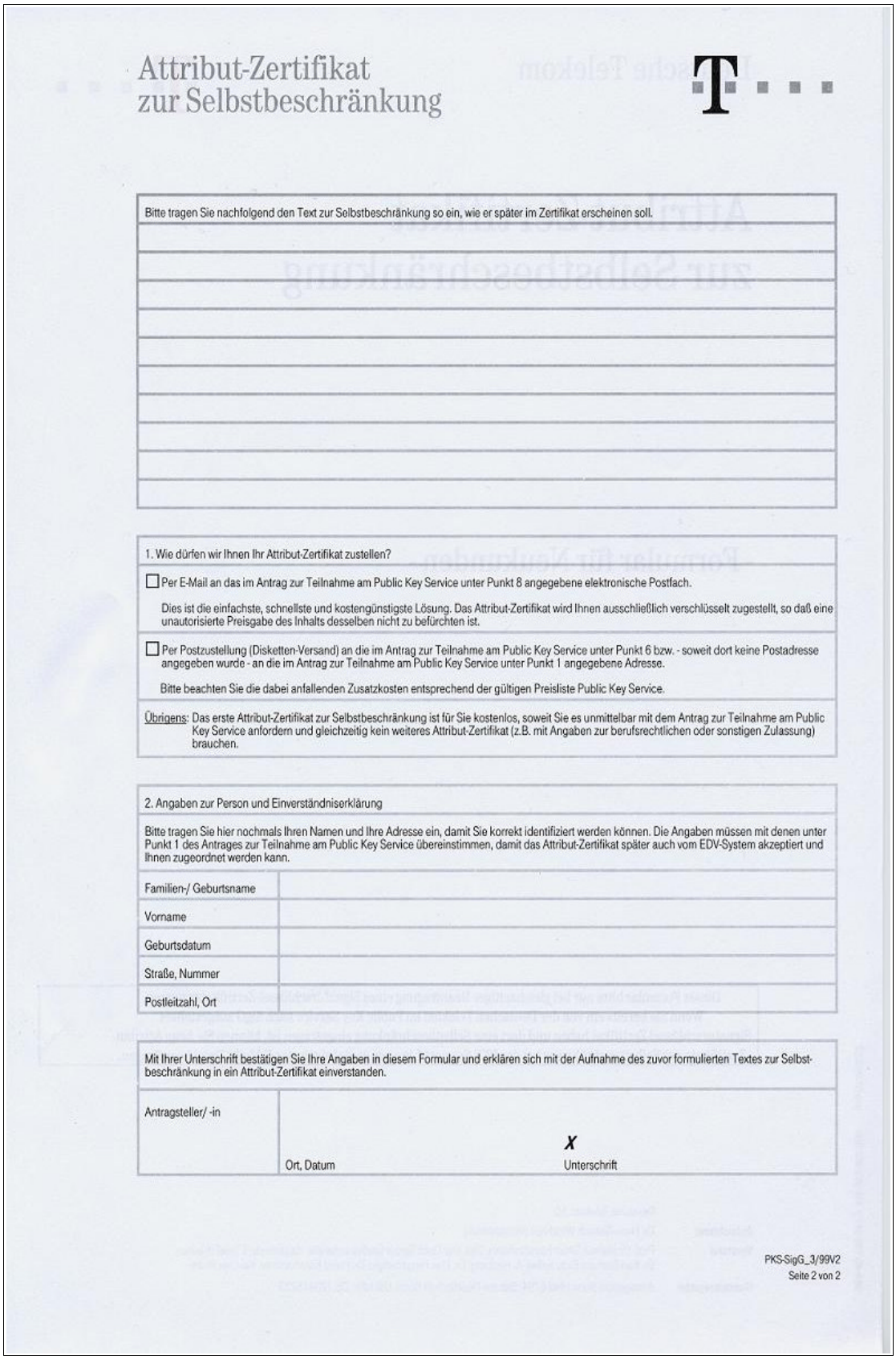
WICHTIG: Leisten Sie Ihre Unterschrift bitte ausschließlich in Anwesenheit eines Mitarbeiters/einer Mitarbeiterin der Registrierungsstelle Ihrer Wahl.

Antragsteller/ -in	Ort, Datum	X Unterschrift
Registrierungsstelle (RS)	Ort, Datum	X Unterschrift RS-Mitarbeiter/ -in

PKS-SigG_3/99V2
Seite 3 von 3

Deutsche Telekom/Trust Center

Abbildung 5.2 Telesec PKS-Antrag Seite 2



Attribut-Zertifikat zur Selbstbeschränkung

Bitte tragen Sie nachfolgend den Text zur Selbstbeschränkung so ein, wie er später im Zertifikat erscheinen soll.

1. Wie dürfen wir Ihnen Ihr Attribut-Zertifikat zustellen?

☐ Per E-Mail an das im Antrag zur Teilnahme am Public Key Service unter Punkt 8 angegebene elektronische Postfach.

Dies ist die einfachste, schnellste und kostengünstigste Lösung. Das Attribut-Zertifikat wird Ihnen ausschließlich verschlüsselt zugestellt, so daß eine unautorisierte Preisgabe des Inhalts desselben nicht zu befürchten ist.

☐ Per Postzustellung (Disketten-Versand) an die im Antrag zur Teilnahme am Public Key Service unter Punkt 6 bzw. - soweit dort keine Postadresse angegeben wurde - an die im Antrag zur Teilnahme am Public Key Service unter Punkt 1 angegebene Adresse.

Bitte beachten Sie die dabei anfallenden Zusatzkosten entsprechend der gültigen Preisliste Public Key Service.

Übrigens: Das erste Attribut-Zertifikat zur Selbstbeschränkung ist für Sie kostenlos, soweit Sie es unmittelbar mit dem Antrag zur Teilnahme am Public Key Service anfordern und gleichzeitig kein weiteres Attribut-Zertifikat (z.B. mit Angaben zur berufsrechtlichen oder sonstigen Zulassung) brauchen.

2. Angaben zur Person und Einverständniserklärung

Bitte tragen Sie hier nochmals Ihren Namen und Ihre Adresse ein, damit Sie korrekt identifiziert werden können. Die Angaben müssen mit denen unter Punkt 1 des Antrages zur Teilnahme am Public Key Service übereinstimmen, damit das Attribut-Zertifikat später auch vom EDV-System akzeptiert und Ihnen zugeordnet werden kann.

Familien-/ Geburtsname	
Vorname	
Geburtsdatum	
Straße, Nummer	
Postleitzahl, Ort	

Mit Ihrer Unterschrift bestätigen Sie Ihre Angaben in diesem Formular und erklären sich mit der Aufnahme des zuvor formulierten Textes zur Selbstbeschränkung in ein Attribut-Zertifikat einverstanden.

Antragsteller/ -in	Ort, Datum	X Unterschrift

PKS-SigG_3/99V2
Seite 2 von 2

Abbildung 5.3 Antrag für Attribut-Zertifikat Selbstbeschränkung

Anhang C – XML Schema für die Archiv-Sicherungsdatei

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- edited with XMLSPY v5 rel. 2 U (http://www.xmlspy.com) by Daniel Ohst  -->
<!--W3C Schema generated by XMLSPY v5 rel. 2 U (http://www.xmlspy.com)-->
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
    <xs:element name="Comment">
        <xs:annotation>
            <xs:documentation>Dieses Feld wird mit dem Grund für die Erstellung der Archiv-Sicherungsdatei versehen. Diese können z.B. die erstmalige Erstellung, Konvertierung in ein neues Zielformat, Änderungen von Metadaten oder Löschen von Dateien.</xs:documentation>
        </xs:annotation>
        <xs:complexType/>
    </xs:element>
    <xs:element name="DigestMethod">
        <xs:annotation>
            <xs:documentation>Hier ist die Angabe  zum für die Referenzierung der Dateien genutzten Hash-Algorithmus einzutragen. Dies erfolgt entsprechend der Empfehlung der W3C Recommendation zu XML-Signaturen. Bei der Auswahl sollen die regelmäßigen Empfehlungen des BSI zu geeigneten Kryptoalgorithmen zugrunde gelegt werden. Der hier verwendete Algorithmus SHA-1 ist bis mindestens Ende 2008 als ausreichend sicher anzusehen und wird mit dem Eintrag http://www.w3.org/2000/09/xmldsig#sha1 referenziert.</xs:documentation>
        </xs:annotation>
        <xs:complexType>
            <xs:attribute name="Algorithm" type="xs:anyURI" use="optional" default="http://www.w3.org/2000/09/xmldsig#sha1 "/>
        </xs:complexType>
    </xs:element>
    <xs:element name="DigestValue">
        <xs:annotation>
            <xs:documentation>Mit einem vertrauenswürdigen und dokumentierten Programm wird der Hash-Wert zur Datei berechnet und BASE64-kodiert eingetragen. </xs:documentation>
        </xs:annotation>
        <xs:complexType/>
    </xs:element>
    <xs:element name="Disclaimer" type="xs:string">
        <xs:annotation>
            <xs:documentation>Enthält den Absatz zum Inhalt und zur Bedeutung der Archiv-Sicherungsdatei.</xs:documentation>
        </xs:annotation>
    </xs:element>
    <xs:element name="DocGroup">
        <xs:annotation>
            <xs:documentation>Das Tag enthält die Zuordnung der Datei zu einer der definierten Dokumentgruppen 'PDF', 'HTML', 'SGML', 'Original' oder 'Metadaten'. Eine Mehrfachzuordnung ist zulässig.
</xs:documentation>
        </xs:annotation>
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:enumeration value="HTML"/>
                <xs:enumeration value="METADATA"/>
                <xs:enumeration value="ORIGINAL"/>
                <xs:enumeration value="PDF"/>
                <xs:enumeration value="SGML"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>
    <xs:element name="MimeType">
        <xs:annotation>
            <xs:documentation>Enthält den MIME-Type der referenzierten Datei. Dieser sollte bei der Implementation eines Tools zur Unterstützung der Erstellung der Archiv-Sicherungsdatei aus der Dateiendung generiert und vorgeschlagen werden. Eine Liste der derzeit verwendeten Typen ist im XML-Schema voreingestellt. Zu diesen existiert auch jeweils die dokumentierte Viewer-Software. Eine Erweiterung ist jedoch jederzeit möglich. </xs:documentation>
        </xs:annotation>
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:enumeration value="application/java"/>
                <xs:enumeration value="application/msword"/>
                <xs:enumeration value="application/octet-stream"/>
```

```
                        <xs:enumeration value="application/pdf"/>
                        <xs:enumeration value="application/postscript"/>
                        <xs:enumeration value="application/wordperfect"/>
                        <xs:enumeration value="application/x-compressed"/>
                        <xs:enumeration value="application/x-latex"/>
                        <xs:enumeration value="audio/mpeg3"/>
                        <xs:enumeration value="audio/wav"/>
                        <xs:enumeration value="image/jpeg"/>
                        <xs:enumeration value="image/png"/>
                        <xs:enumeration value="model/vrml"/>
                        <xs:enumeration value="text/css"/>
                        <xs:enumeration value="text/html"/>
                        <xs:enumeration value="text/plain"/>
                        <xs:enumeration value="text/richtext"/>
                        <xs:enumeration value="text/sgml"/>
                        <xs:enumeration value="text/xml"/>
                        <xs:enumeration value="video/avi"/>
                        <xs:enumeration value="video/mpeg"/>
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
            <xs:element name="archive">
                <xs:annotation>
                    <xs:documentation>Start-Tag für das gesamte Paket</xs:documentation>
                </xs:annotation>
                <xs:complexType>
                    <xs:sequence>
                        <xs:element ref="urn"/>
                        <xs:element ref="counter"/>
                        <xs:element ref="date"/>
                        <xs:element ref="contact"/>
                        <xs:element ref="documentType" maxOccurs="unbounded"/>
                        <xs:element ref="title"/>
                        <xs:element ref="author"/>
                        <xs:element ref="DigestMethod"/>
                        <xs:element ref="file"/>
                        <xs:element ref="Comment"/>
                        <xs:element ref="Disclaimer"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="author">
                <xs:annotation>
                    <xs:documentation>Es wird der bzw. die Autor(en) der Publikation eingetragen.
</xs:documentation>
                </xs:annotation>
                <xs:complexType/>
            </xs:element>
            <xs:element name="contact" type="xs:string">
                <xs:annotation>
                    <xs:documentation>Hier wird die jeweils aktuelle Anschrift der „Arbeitsgruppe Elektronisches
Publizieren“, insbesondere die Email-Adresse eingetragen. Da die Archiv-Sicherungsdatei auch veröffentlicht werden kann,
wird hier den Nutzern die Möglichkeit gegeben, bei eventuellen Fragen Kontakt aufzunehmen. </xs:documentation>
                </xs:annotation>
            </xs:element>
            <xs:element name="counter">
                <xs:annotation>
                    <xs:documentation>Enthält eine Zahl beginnend mit 1 und stellt damit eine Chronologie zwischen
den ASDs her. Die Zahl bezieht sich gleichzeitig auf das Verzeichnis der Archiv-Ordnerstruktur, die gerade bearbeitet
wird.</xs:documentation>
                </xs:annotation>
                <xs:complexType/>
            </xs:element>
            <xs:element name="date">
                <xs:annotation>
                    <xs:documentation>Das Erstellungsdatum der Archiv-Sicherungsdatei wird im Format ISO
8601:2000 [ISO00a] eingetragen, z.B. 2003-06-25. </xs:documentation>
                </xs:annotation>
                <xs:complexType/>
            </xs:element>
            <xs:element name="documentType">
```

```
            <xs:annotation>
                <xs:documentation>Dieses Tag stellt den Typ der Publikation dar. Derzeit ist einer der Werte
'Dissertation', 'Habilitation', 'Vorlesung' ,'Diplom/Magisterarbeit', 'Zeitschrift', 'Monographie', 'Sonstige'. Alternativ
könnten auch die englischen Begriffe verwendet werden, um die Einheitlichkeit zu erhöhen. </xs:documentation>
            </xs:annotation>
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:enumeration value="Diplom/Magisterarbeit"/>
                    <xs:enumeration value="Dissertation"/>
                    <xs:enumeration value="Habilitation"/>
                    <xs:enumeration value="Monographie"/>
                    <xs:enumeration value="Sonstige"/>
                    <xs:enumeration value="Vorlesung"/>
                    <xs:enumeration value="Zeitschrift"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="file">
            <xs:annotation>
                <xs:documentation>Start-Tag für jede Datei des Dokuments</xs:documentation>
            </xs:annotation>
            <xs:complexType>
                <xs:sequence>
                    <xs:element ref="uri"/>
                    <xs:element ref="MimeType" maxOccurs="unbounded"/>
                    <xs:element ref="DocGroup" maxOccurs="unbounded"/>
                    <xs:element ref="DigestValue"/>
                </xs:sequence>
            </xs:complexType>
        </xs:element>
        <xs:element name="title">
            <xs:annotation>
                <xs:documentation>Es wird der Titel der Publikation eingetragen.</xs:documentation>
            </xs:annotation>
            <xs:complexType/>
        </xs:element>
        <xs:element name="uri">
            <xs:annotation>
                <xs:documentation>Referenz auf die Datei. Diese wird derzeit als relativer Pfad innerhalb der
Ordnerstruktur des Dokuments unterhalb des URN angegeben.</xs:documentation>
            </xs:annotation>
            <xs:complexType/>
        </xs:element>
        <xs:element name="urn">
            <xs:annotation>
                <xs:documentation>Bereits bei der Abgabe einer Publikation sollte aus dem Pool ein URN
bestimmt werden, der ab diesem Zeitpunkt zur allgemeinen Identifizierung genutzt wird. Das Präfix des URN wird weder
in der XML-Datei noch bei der Benennung der Archiv-Sicherungsdatei verwendet.</xs:documentation>
            </xs:annotation>
            <xs:complexType/>
        </xs:element>
    </xs:schema>
```

Anhang D – XML-Schema Archiv-Sicherungsdatei für Migration alter Dokumente

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!-- edited with XMLSPY v5 rel. 2 U (http://www.xmlspy.com) by Daniel Ohst (HiSolutions) -->
<!--W3C Schema generated by XMLSPY v5 rel. 2 U (http://www.xmlspy.com)-->
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
    <xs:element name="Comment">
        <xs:annotation>
            <xs:documentation>Migration eines Dokuments.</xs:documentation>
        </xs:annotation>
        <xs:complexType/>
    </xs:element>
    <xs:element name="DigestMethod">
        <xs:annotation>
            <xs:documentation>Hier ist die Angabe  zum für die Referenzierung der Dateien genutzten Hash-Algorithmus einzutragen. Dies erfolgt entsprechend der Empfehlung der W3C Recommendation zu XML-Signaturen. Bei der Auswahl sollen die regelmäßigen Empfehlungen des BSI zu geeigneten Kryptoalgorithmen zugrunde gelegt werden. Der hier verwendete Algorithmus SHA-1 ist bis mindestens Ende 2008 als ausreichend sicher anzusehen und wird mit dem Eintrag http://www.w3.org/2000/09/xmldsig#sha1 referenziert.</xs:documentation>
        </xs:annotation>
        <xs:complexType>
            <xs:attribute name="Algorithm" type="xs:anyURI" use="optional" default="http://www.w3.org/2000/09/xmldsig#sha1 "/>
        </xs:complexType>
    </xs:element>
    <xs:element name="DigestValue">
        <xs:annotation>
            <xs:documentation>Mit einem vertrauenswürdigen und entsprechend dokumentierten Programm wird der Hash-Wert zur Datei berechnet und BASE64-kodiert eingetragen. </xs:documentation>
        </xs:annotation>
        <xs:complexType/>
    </xs:element>
    <xs:element name="Disclaimer" type="xs:string">
        <xs:annotation>
            <xs:documentation>Dies ist eine eingeschränkte Archiv-Sicherungsdatei für Dokumente zu Migrationszwecken.</xs:documentation>
        </xs:annotation>
    </xs:element>
    <xs:element name="archive">
        <xs:annotation>
            <xs:documentation>Start-Tag für das gesamte Paket</xs:documentation>
        </xs:annotation>
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="urn" minOccurs="0"/>
                <xs:element ref="date"/>
                <xs:element ref="contact"/>
                <xs:element ref="archivename"/>
                <xs:element ref="DigestMethod"/>
                <xs:element ref="file"/>
                <xs:element ref="Comment"/>
                <xs:element ref="Disclaimer"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="contact" type="xs:string">
        <xs:annotation>
            <xs:documentation>Hier wird die jeweils aktuelle Anschrift der „Arbeitsgruppe Elektronisches Publizieren“, insbesondere die Email-Adresse, eingetragen. Da die Archiv-Sicherungsdatei auch veröffentlicht werden kann, wird hier den Nutzern die Möglichkeit gegeben, bei eventuellen Fragen Kontakt aufzunehmen. </xs:documentation>
        </xs:annotation>
    </xs:element>
    <xs:element name="date">
        <xs:annotation>
            <xs:documentation>Das Erstellungsdatum der Archiv-Sicherungsdatei wird im ISO 8601:2000 Format [ISO00a] eingetragen, z.B. 2003-06-25. </xs:documentation>
        </xs:annotation>
        <xs:complexType/>
```

```
    </xs:element>
    <xs:element name="file">
        <xs:annotation>
            <xs:documentation>Start-Tag für jede Datei des Dokuments</xs:documentation>
        </xs:annotation>
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="uri"/>
                <xs:element ref="DigestValue"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="archivename">
        <xs:annotation>
            <xs:documentation>Es wird der Name des Ordners auf dem Archivserver eingetragen.</xs:documentation>
        </xs:annotation>
        <xs:complexType/>
    </xs:element>
    <xs:element name="uri">
        <xs:annotation>
            <xs:documentation>Referenz auf die Datei. Diese wird derzeit als relativer Pfad innerhalb der Ordnerstruktur
des Dokuments unterhalb des URN angegeben.</xs:documentation>
        </xs:annotation>
        <xs:complexType/>
    </xs:element>
    <xs:element name="urn">
        <xs:annotation>
            <xs:documentation>Falls ein URN für das Dokument existiert kann, dieser hier eingetragen
werden.</xs:documentation>
        </xs:annotation>
        <xs:complexType/>
    </xs:element>
</xs:schema>
```

Anhang E – Beispiel Präsentationsproblem

Das folgende Beispiel illustriert recht deutlich die Auswirkungen des Präsentationsproblems und ist zudem ein real vorgekommener Fall. Hintergrund ist eine Anfrage an den Service des Betreibers einer großen Online-Handelsplattform für Kraftfahrzeuge. In einem geschlossenen Nutzerbereich gibt es einen Button „Abmeldung“, der nicht - wie analog zu vielen anderen Angeboten im Internet - ein sicheres Verlassen des Bereichs ermöglicht, sondern die Auflösung des Vertrages mit dem Anbieter einleitet. Zwar wird auf der erscheinenden Seite darauf hingewiesen, dass die endgültige Abmeldung erst nach einer Bestätigungsmail erfolgt, aber der Text suggeriert weiterhin, dass wohl unmittelbar die Vertriebsabteilung eingeschaltet wird, um die Gründe für die Abmeldung zu erfahren und den Kunden doch zum Bleiben zu überreden. Auf die Mail an den Service des Betreibers mit dem Hinweis auf die verwirrende Funktion und der Bitte, die Abmeldung natürlich nicht einzuleiten, kam folgende Antwortmail, die im ersten Screenshot in der Outlook-Voransicht dargestellt wird.

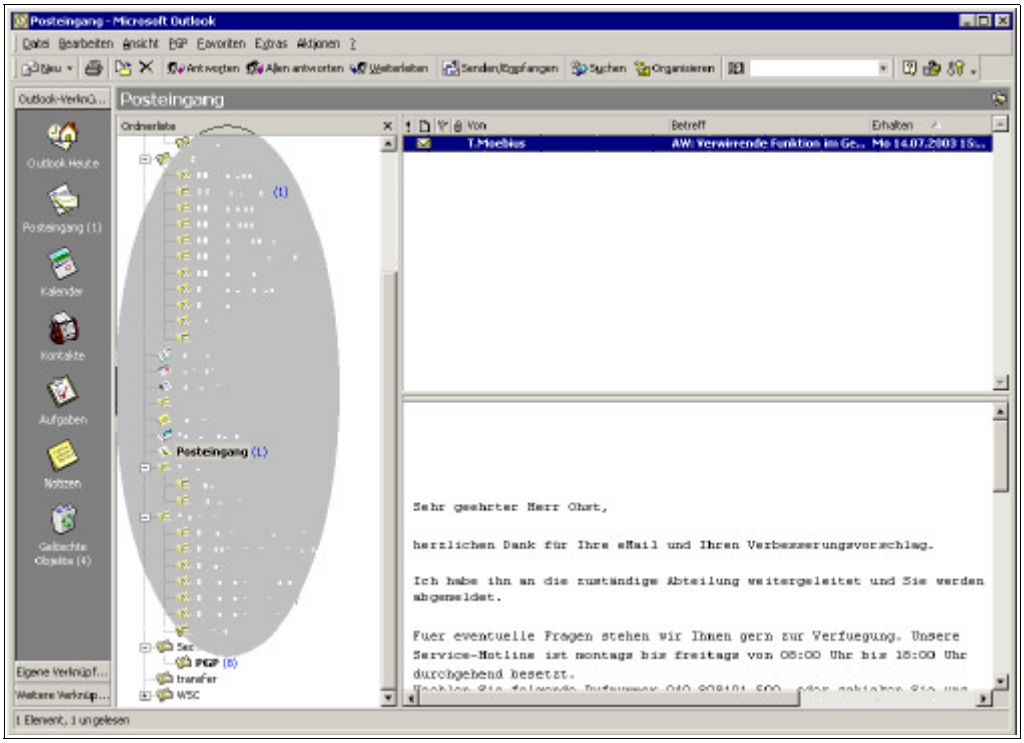


Abbildung 5.4 Präsentationsproblem 1

Der Satz, der in dieser Ansicht zu lesen ist, lautet: „... Ich habe ihn an die zuständige Abteilung weitergeleitet und Sie werden abgemeldet.“ Dies entspricht natürlich überhaupt nicht der gewünschten Reaktion. Es ist nicht ohne weiteres zu erkennen, dass der

Satz an dieser Stelle weitergeht, man müsste schon genau auf die Scrollbars achten. Der nachfolgende Screenshot enthält die vollständig geöffnete Mail. Hier ist der komplette Satz zu sehen, der eine völlig andere Bedeutung ergibt.

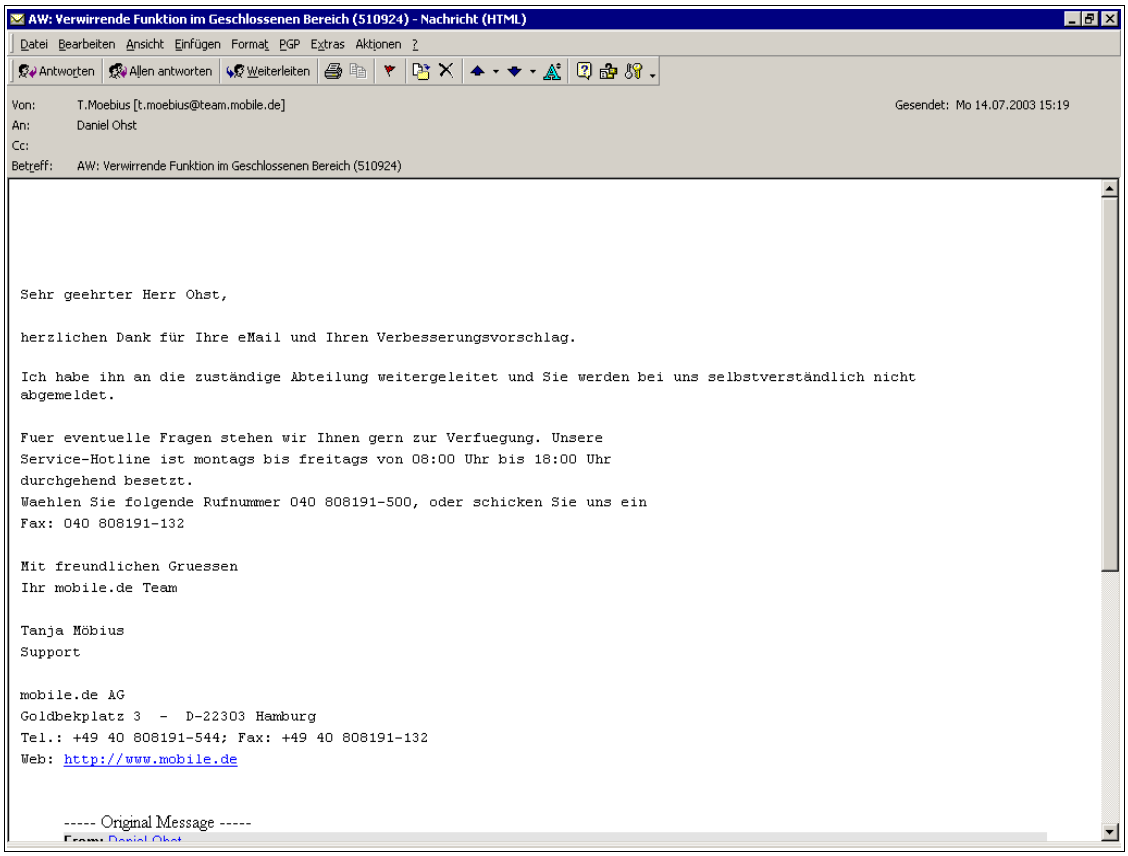


Abbildung 5.5 Präsentationsproblem 2

Auch wenn in diesem Beispiel elektronische Signaturen keine Rolle gespielt haben, wird doch deutlich, dass es von großer Bedeutung ist, auf geeignete Weise den Inhalt des zu signierenden Dokuments darzustellen, da ansonsten u.U. das genaue Gegenteil der gewünschten Aussage unterschrieben wird.

Literaturverzeichnis

[ApvrilleG02] Axelle Apvrille, Vincent Girier: XML Security Time Stamping Protocol, 2002.

[BMF01] Bundesministerium der Finanzen: Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen.

[BNotK98] Bundesnotarkammer: Mitwirkung von Notaren bei der Erteilung von Attribut-Zertifikaten nach §§ 5 Abs. 2, 7 Abs. 2 SigG. 1998, Rundschreiben Nr. 47/98.

[Brandner02] Ralf Brandner: Langzeitarchivierung elektronisch signierter Dokumente – Rechtliche und anwendungsorientierte Anforderungen und Lösungen im Bereich des Gesundheitswesens, 2002.

[BrandnerPRS02] Ralf Brandner, Ulrich Pordesch, Alexander Roßnagel, Joachim Schachermayer: Langzeitsicherung qualifzierter elektronischer Signaturen. 2002, DuD 26

[BrandnerS02] Ralf Brandner, Paul Schmücker: Die neue Gesetzgebung zur Digitalen Signatur und Archivierung – welche Möglichkeiten bieten digitale Signaturen im Gesundheitswesen?, KIS 2002.

[BrandnerP03] Ralf Brandner, Ulrich Pordesch: Konzept zur signaturgesetzkonformen Erneuerung qualifizierter Signaturen. DuD 6/2003.

[BSI97] Bundesamt für Sicherheit in der Informationstechnik: BSI-Handbuch für digitale Signaturen auf Grundlage von SigG und SigV 97. 1997

[BSI00] Bundesamt für Sicherheit in der Informationstechnik: Signatur-Interoperabilitätsspezifikation SigI. 2000,
http://www.bsi.de/esig/basics/techbas/interop/bsi/sigib4.pdf

[Clayton01] Richard Clayton: Brute Force Attacks on Cryptographic Keys. 2001.
http://www.cl.cam.ac.uk/users/rnc1/brute.html

[DBV01] Deutscher Bibliotheksverband: Stellungnahme des DBV zum Strategiekonzept „Zukunft der wissenschaftlichen und technischen Information. 2001

[DDBa] Die Deutsche Bibliothek: Der Sammelauftrag.

[DDB02b] Deutsch Bibliothek, RZ u. UB HU-Berlin, SUB Göttingen, Bayerische Staatsbibliothek München: Arbeitspapier zum Workshop

[DINI02] Deutsche Initiative für Netzwerkinformation: Empfehlungen zum elektronischen Publizieren. 2002

[Dittmann] Jana Dittmann: Urheberschutz: Elektronische Signaturen als Wasserzeichen. o.J.

[DFG95] Deutsche Forschungsgemeinschaft: Elektronische Publikationen im Literatur- und Informationsangebot wissenschaftlicher Bibliotheken. 1995

[Dobratz02] Susanne Dobratz: Langzeitarchivierung elektronischer Dokumente. 2002, Sun Summit Digitale Bibliotheken Frankfurt.

[DobratzT02] Susanne Dobratz, Inka Tappenbeck: Thesen zur Zukunft der digitalen Langzeitarchivierung in Deutschland. 2002, Bibliothek 3

[EDOC01a] Arbeitsgruppe Elektronisches Publizieren: Leitlinien für den Betrieb des Dokumentenservers. 2001 http://edoc.hu-berlin.de/e_info/leitlinien.php

[EDOC02a] Hinweise zur Abgabe von Dissertationen für Promovenden.

[EDOC03a] Projekte der Arbeitsgruppe Elektronisches Publizieren. 2003. http://edoc.hu-berlin.de/e_projekte/

[ETSI02a] ETSI: XML Advanced Electronic Signatures, ETSI TS 101 903 V1.1.1. 2002.

[Fiedler03] Arno Fiedler: ISIS-MTT Interoperable PKI-Anwendungen. Präsentation BITS 4/2003.

[FISCHER-DIESKAUGPS02] Stephanie Fischer-Dieskau, Rotraud Gitter, Sandra Paul, Roland Steidle: Elektronisch signierte Dokumente als Beweismittel im Zivilprozess, 2002.

[FormAnpG01] Bundesgesetzblatt: Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr. 2001, Teil I Nr. 35

[Forret02] Peter Forret: Digital Receipts, ISSE 2002.

[Geis01] Ivo Geis: Rechtsaspekte elektronischer Geschäftsbeziehungen. 2001

[GIITG02] Gesellschaft für Informatik, Informationstechnische Gesellschaft: Memorandum zur Förderung des elektronischen Rechts- und Geschäftsverkehrs. 2002

[Hirsch02] Frederick Hirsch: Getting started with XML Security, http://www.fjhirsch.com/xml/xmlsec/starting-xml-security.html 2002.

[HIS03] HiSolutions AG: Präsentation Elektronische Signaturen. 2003

[HU99] Humboldt-Universität zu Berlin: Habiltationsordung der Medizinischen Fakultät Charité. 1999 in Amtliches Mitteilungsblatt 02/99.

[HUAS98] Akademischer Senat der Humboldt-Universität zu Berlin: Beschluss zur elektronischen Veröffentlichung von Dissertationen.

[IETF03] C. Wallace, S. Chokhani: Internet Draft „Trusted Archive Protocol“. 2003

[ISO00] International Standards Organization: ISO8601:2000(E) – Representation of Dates and Times. 2000

[Jungermann02] Sebastian Jungermann: Der Beweiswert elektronischer Signaturen. 2002

[Kelm02] Stefan Kelm: Signaturgesetz, quo vadis?, 2002, 9. DFN-CERT Workshop.

[KES02a] KES: Digitale Signatur – Akkreditierung ohne Zukunft?, KES 3/2002 S. 24

[KMK97] Kultusministerkonferenz: Grundsätze für die Veröffentlichung von Dissertationen. 1997

[LangenbachU2002] C.J.Langenbach, O.Ulrich (Hrsg.): Elektronische Signaturen – Kulturelle Rahmenbedingungen einer technischen Entwicklung. 2002

[Maseberg02] Jan Sönke Maseberg: Fail Safe Konzept für Public Key Infrastrukturen. 2002

[Mertens00] Frank Mertens: Entwicklung eines Computerprogramms zur Durchführung elektronischer Setups. Dissertation HU Berlin 2000

[METS03]: Library of Congress: Metadata Encoding and Transmission Standard. 2003, http://www.loc.gov/standards/mets/

[MWFKBW99] Empfehlungen zum Aufbau einer Servernetzwerks für elektronische Hochschulpublikationen. 1999

[OIAS02] Consultative Committee for Space Data Systems: Reference Model for an Open Archival Information Systems. 2002

[Pinkas02] Denis Pinkas: Timestamping for 30 years ... and more. ISSE 2002.

[ProPrint03] Projekt Proprint.

[Rapp02] Christiane Rapp: Rechtliche Rahmenbedingungen und Formqualität elektronischer Signaturen. 2002

[RegTP01] RegTP: Geeignete Kryptoalgorithmen, 2003

[RegTP01b] RegTP: Fachgespräch „Technik und Recht der elektronischen Signaturen“. 2001

[RegTP02a] RegTP: Einheitliche Spezifizierung der Einsatzbedingungen´für Signaturanwendungskomponenten. 2002

[RegTP03a] RegTP: Produkte für qualifizierte elektronische Signaturen. 2003. http://www.regtp.de/tech_reg_tele/start/in_06-02-05-00-00_m/index.html

[Reimer02] Helmut Reimer: ISIS-MTT – Interoperable PKI-Anwendungen. 2002

[RFC96a] Multipurpose Internet Mail Extensions. http://www.ietf.org/rfc/rfc2046.txt

[RFC98a] Uniform Resource Identifiers (URI): Generic Syntax. http://www.ietf.org/rfc/rfc2396.txt

[Rossnagel03a] Alexander Roßnagel: Das elektronische Verwaltungsverfahren. 2003, NJW 469-476

[Rossnagel03b] Alexander Roßnagel: Die fortgeschrittene elektronische Signatur. In Multimedia und Recht 03/2003.

[RossnagelFDPB03c] Alexander Roßnagel, Stefanie Fischer-Dieskau, Ulrich Pordesch, Ralf Brandner: „Erneuerung elektronischer Signaturen“. In Computer & Recht 04/2003.

[SigG01] Bundesgesetzblatt: Gesetz über Rahmenbedingungen für elektronische Signaturen. 2001

[SigRL00] Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen. 2000.

[SigV01] Bundesgesetzblatt: Verordnung zur elektronischen Signatur. 2001

[Splittgerber03] Splittgerber: Die elektronische Form von bestimmenden Schriftsätzen. In Computer & Recht 01/2003.

[StDÜV03] Bundesgesetzblatt: Steuerdaten-Übermittlungsverordnung. 2003, Teil I Nr 5.

[StÄndG01] Bundesgesetzblatt: Gesetz zur Änderung steuerlicher Vorschriften. 2001, Teil I Nr. 72.

[TC03] TC Trustcenter AG: Trustcenter News – Startschuss für Projekt Sichere Signaturinfrastruktur. 4/2003.

[UHG03] Ein Artikel zum neuen Urheberrechtsgesetz und der politischen Debatte dazu.

[UBDO03] Universitätsbibliothek Dortmund: ELDORADO FAQ. 2003, http://eldorado.uni-dortmund.de:8080/faq/faq.html

[VerwVerfAendG02] Bundesgesetzblatz: Drittes Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften. 2002, Teil I Nr. 60

[W3C02a] W3C: XML-Signature Syntax and Processing. W3C Recommendation 12 February 2002. http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

[W3C03a] W3C: XML Advanced Electronic Signatures (XadES). W3C Note 20/02/03. http://www.w3.org/TR/2003/NOTE-XAdES-20030220/

[Wendland02] Bert Wendland: Braucht ein Dokumentenserver eine Policy?. 2002, Bibliotheksdienst 2002, 741-746

[WR01] Wissenschaftsrat: Empfehlungen zur digitalen Informationsversorgung durch Hochschulbibliotheken. 2001

Danksagung

Ich möchte zunächst bei Prof. Wolfgang Coy, Prof. Ernst-Günter Giessmann und Dr. Schirmbacher für die Begutachtung der Arbeit und für ihre Unterstützung bedanken, die wesentlich zum Entstehen dieser Arbeit beigetragen hat.

Mein Dank gilt den Mitarbeitern des Computer- und Medienservice der HU Berlin, die durch ihre Hilfe und Anregungen zur Entwicklung des Konzepts beigetragen haben, insbesondere Susanne Dobratz, Uwe Müller, Matthias Schulz und Bert Wendland.

Weiterhin möchte ich Ulrike Schulte (Teletrust e.V.) für die unkomplizierte Bereitstellung der Präsentationen, Volker Mann (Telesec) für die wertvollen Informationen zu Fragen des Zertifizierungsdienstes sowie Dr. Bruno Klotz-Berendes (UB Dortmund) für das aufschlussreiche Gespräch zur Entwicklung im Bibliotheksbereich danken.

Meiner Familie gilt mein Dank für die tatkräftige Unterstützung bei der Fertigstellung dieser Diplomarbeit.

Selbständigkeitserklärung

Hiermit erkläre ich, dass ich die vorgelegte Diplomarbeit eigenständig und ohne die unzulässige Hilfe Dritter verfasst habe. Die benutzten Hilfsmittel sowie die Literatur wurden vollständig angegeben.

Berlin, den 01.09.2003

Daniel Ohst